



## Syberkey MarineAuth Product Platform

### Maritime Verified Identity, Action and Document Trust Platform

**MarineAuth protects ships, ports and logistics networks by ensuring that high-risk maritime actions are approved only by verified authorised people or governed AI agents. It combines biometric identity, continuous policy enforcement, document verification, verified communications, vendor access control and AI Airlock governance into a standalone maritime trust platform.**

### Product Explanation Document

#### 1. Executive Summary

**MarineAuth** is a standalone maritime trust and cybersecurity product Platform built on SyberKey/OneBioID technology. It is designed to verify the **real person, role, document, instruction, vendor, privileged action or AI agent** before a maritime transaction, cargo release, port approval, ship-shore access or operational command is allowed to proceed.

MarineAuth is not just an authentication tool and it is not another generic maritime cybersecurity monitoring system. Its purpose is more specific and commercially powerful:

**MarineAuth verifies and certifies trusted maritime actions before cargo, documents, instructions, remote access or AI-driven decisions are released.**

The product is especially suited to maritime environments because the industry depends on high-trust actions across many disconnected or semi-connected parties: ship owners, ship managers, captains, chief engineers, shipping agents, freight

forwarders, port authorities, terminal operators, customs brokers, insurers, banks, contractors, vendors and emerging AI systems.

MarineAuth creates a **verified chain of trust** across these parties.

It can be used for:

- cargo release verification;
- bill of lading and delivery order verification;
- biometric maritime document signing;
- verified maritime email and shipping instructions;
- remote vendor access to vessels and port systems;
- privileged command approvals;
- captain/chief engineer approvals;
- port terminal override approvals;
- AI agent identity and AI Airlock control;
- audit-ready Human Action Certificates.

The product's main message is simple:

**Nothing critical moves in maritime unless the right verified person, document, instruction or AI agent has approved it.**

## 2. The Problem MarineAuth Solves

The maritime industry is becoming highly digital, but trust is still often based on weak or fragmented methods:

- email instructions;
- scanned documents;
- passwords;
- OTPs;
- manual signatures;
- PDF attachments;
- shared vendor credentials;
- port system logins;

- VPN access;
- paper-based approval trails;
- unverified AI recommendations.

This creates several serious risks.

### **2.1 Cargo Release Fraud**

Cargo can be released based on forged documents, compromised emails, fake shipping agents or manipulated delivery instructions. Once cargo leaves a terminal, recovery can be difficult and losses can be significant.

### **2.2 Bill of Lading and Document Fraud**

Maritime trade depends on documents such as bills of lading, sea waybills, cargo release orders, letters of indemnity, port clearance documents and delivery orders. These documents can be forged, altered, copied or misused.

### **2.3 Business Email Compromise**

Maritime operations still rely heavily on email. Fraudsters can impersonate shipping agents, port authorities, freight forwarders, customers or payment teams to send false instructions.

Examples include:

- “release this cargo”;
- “change the bank account”;
- “approve this invoice”;
- “accept this delivery order”;
- “authorise this vendor”;
- “approve this port charge”.

### **2.4 Remote Vendor Access Risk**

Ships and ports depend heavily on remote vendors for engines, navigation systems, satellite communications, cranes, terminal systems, IT support and OT maintenance. If vendor access is not strongly controlled, it can become a major cybersecurity risk.

### **2.5 Port and Terminal Operational Risk**

Port and terminal systems control gates, cranes, container yards, cargo release, truck appointments, dangerous goods handling and terminal operating systems. A wrong or unauthorised action can cause commercial loss, safety risk or supply-chain disruption.

## 2.6 AI Governance Risk

Maritime AI systems are emerging for route optimisation, fuel optimisation, predictive maintenance, port scheduling, cargo planning, customs documentation and cyber incident response. These AI agents need identity, boundaries and verified human approval before they influence or execute critical actions.

MarineAuth addresses these risks by verifying the human or AI authority behind the action before the action is accepted.

## 3. What MarineAuth Is

MarineAuth is a **Maritime Verified Action Platform**.

It combines the following SyberKey/OneBioID technologies into a maritime-specific product:

| SyberKey / OneBioID Capability | MarineAuth Application                                         |
|--------------------------------|----------------------------------------------------------------|
| BioAuth / OneBioID             | Verifies maritime users biometrically                          |
| QR-based digital Bio-ID        | Portable maritime identity credential                          |
| Live biometric step-up         | Confirms the real person at high-risk action time              |
| Passwordless SSO / IAP         | Secure login to maritime portals and systems                   |
| Adaptive MFA                   | Risk-based authentication by role, device, location and action |
| CPE                            | Continuous Pathway Enforcement from login to execution         |
| Bio-PAM / PRN                  | Privileged vendor and admin access approval                    |
| FingerSign                     | Biometric maritime document signing                            |
| VerifiedBioMail                | Verified maritime email and shipping instructions              |

| SyberKey / OneBioID Capability | MarineAuth Application                            |
|--------------------------------|---------------------------------------------------|
| AI Agent Identity              | Synthetic identity for maritime AI agents         |
| AI Airlock                     | Blocks AI execution until verified human approval |
| PQKey                          | Future-resilient cryptographic trust layer        |
| Human Action Certificate       | Proof of verified approval and execution          |

MarineAuth can sit on top of existing maritime systems. It does not require shipping lines, ports or logistics companies to replace their current platforms.

It can integrate with:

- terminal operating systems;
- port community systems;
- shipping line portals;
- freight forwarding systems;
- cargo release platforms;
- email systems;
- Microsoft Entra;
- CyberArk, ARCON or BeyondTrust;
- vessel management systems;
- remote maintenance systems;
- document management systems;
- AI route/fleet systems;
- SOC/SIEM platforms.

## 4. MarineAuth Product Modules

### Module 1: MarineAuth Cargo Release

#### Purpose

To prevent unauthorised or fraudulent cargo release by requiring verified human authority before release instructions are accepted.

## How it works

1. A shipping agent, carrier, freight forwarder or authorised maritime user creates a cargo release request.
2. MarineAuth checks the person's identity, organisation and role.
3. CPE evaluates the cargo, document, terminal, consignee, value and risk level.
4. If required, the user completes BioAuth or live biometric verification.
5. FingerSign signs the cargo release document.
6. A QR verification certificate is generated.
7. The terminal, port or logistics party verifies the certificate before release.
8. MarineAuth issues a Human Action Certificate.

## Value

MarineAuth Cargo Release gives ports, terminals, shipping lines and logistics parties a strong method to verify that a release instruction came from the right person with the right authority.

## Module 2: MarineAuth Document Trust

### Purpose

To create biometric verification and tamper-proof certification for maritime documents.

### Supported documents

MarineAuth can be used for:

- bill of lading;
- sea waybill;
- cargo release order;
- delivery order;
- telex release;
- letter of indemnity;
- dangerous goods declaration;
- port clearance;

- bunker delivery note;
- ship inspection report;
- crew change approval;
- charterparty document;
- customs declaration;
- insurance certificate;
- trade finance document.

### **How it works**

1. User uploads or prepares a maritime document.
2. MarineAuth creates a cryptographic hash of the document.
3. The authorised signer completes BioAuth.
4. For high-risk documents, live biometric step-up is required.
5. FingerSign applies a biometric signing event.
6. A QR verification certificate is attached or linked.
7. Any recipient can verify the document and signer through MarineAuth.
8. If the document is altered, verification fails.

### **Value**

MarineAuth Document Trust creates stronger proof than ordinary e-signature because it links the document to a verified maritime identity, role and biometric approval event.

## **Module 3: MarineAuth Verified Instructions**

### **Purpose**

To stop fraudulent or spoofed maritime instructions sent through email, portals or messaging workflows.

### **Typical verified instructions**

- release cargo;
- change bank details;
- approve payment;

- approve port charges;
- accept delivery order;
- authorise vendor access;
- confirm consignee details;
- approve demurrage or detention charges;
- approve dangerous goods handling;
- approve crew change;
- accept AI-generated operational recommendation.

### **How it works**

1. Sender prepares a high-risk instruction.
2. MarineAuth classifies the instruction type and risk level.
3. CPE checks whether the sender has authority.
4. Sender completes BioAuth or live biometric step-up.
5. The instruction is sent with a verification link or QR certificate.
6. Recipient verifies the sender, organisation, role and approval status.
7. MarineAuth creates a Human Action Certificate.

### **Value**

MarineAuth Verified Instructions helps reduce business email compromise, payment redirection fraud, fake cargo release instructions and impersonation of maritime authorities.

## **Module 4: MarineAuth Vendor Access**

### **Purpose**

To secure remote access by vendors, contractors and service providers to vessel, port, terminal or logistics systems.

### **Typical vendor access scenarios**

- engine OEM remote maintenance;
- ECDIS/navigation software support;
- satellite communications configuration;



- crane system maintenance;
- terminal operating system administration;
- firewall/VPN configuration;
- port gate system support;
- reefer monitoring system access;
- vessel IT support;
- cyber incident response access.

### **How it works**

1. Vendor requests access to a vessel, port or system.
2. MarineAuth verifies the vendor's identity.
3. CPE checks the ticket, time window, asset, role, device and risk.
4. Captain, chief engineer, fleet manager or port supervisor receives approval request.
5. Approver completes BioAuth.
6. MarineAuth issues a time-bound access token.
7. High-risk commands require additional live biometric approval.
8. Human Action Certificate records the session and approval trail.

### **Value**

MarineAuth Vendor Access converts remote maritime support from a password/VPN trust model into a verified, time-bound, biometric approval model.

## **Module 5: MarineAuth Privileged Action Control**

### **Purpose**

To control high-risk actions inside port, vessel, terminal and logistics systems.

### **Examples of privileged actions**

- release container hold;
- override gate rule;
- approve dangerous goods movement;

- change terminal operating system configuration;
- restart vessel monitoring system;
- approve emergency route change;
- grant privileged vendor session;
- alter consignee or cargo release details;
- change bank account for freight payment;
- approve critical maintenance action.

### **How it works**

1. User attempts a high-risk action.
2. MarineAuth CPE intercepts or evaluates the action.
3. CPE determines whether the action is permitted, blocked or requires step-up.
4. User or supervisor completes BioAuth.
5. Dual approval can be required for critical actions.
6. Action is released only after approval.
7. Human Action Certificate is generated.

### **Value**

This gives maritime operators control not only over login, but over the actual execution of sensitive actions.

## **Module 6: MarineAuth AI Agent Control**

### **Purpose**

To govern maritime AI agents and prevent them from executing critical actions without approved human oversight.

### **AI use cases**

- route optimisation;
- fuel optimisation;
- predictive maintenance;
- cargo planning;

- port berth scheduling;
- customs documentation;
- incident response;
- operational risk scoring;
- autonomous or semi-autonomous vessel workflows.

### **How it works**

1. Maritime AI agent is registered in MarineAuth.
2. AI agent is assigned a synthetic identity.
3. AI identity is bound to a verified human sponsor.
4. Allowed and prohibited actions are defined.
5. AI submits a recommendation or execution request.
6. AI Airlock checks whether the action is allowed.
7. If critical, Airlock blocks execution pending verified human approval.
8. Captain, fleet manager or authorised officer approves with BioAuth.
9. MarineAuth records the full AI-to-human approval path.

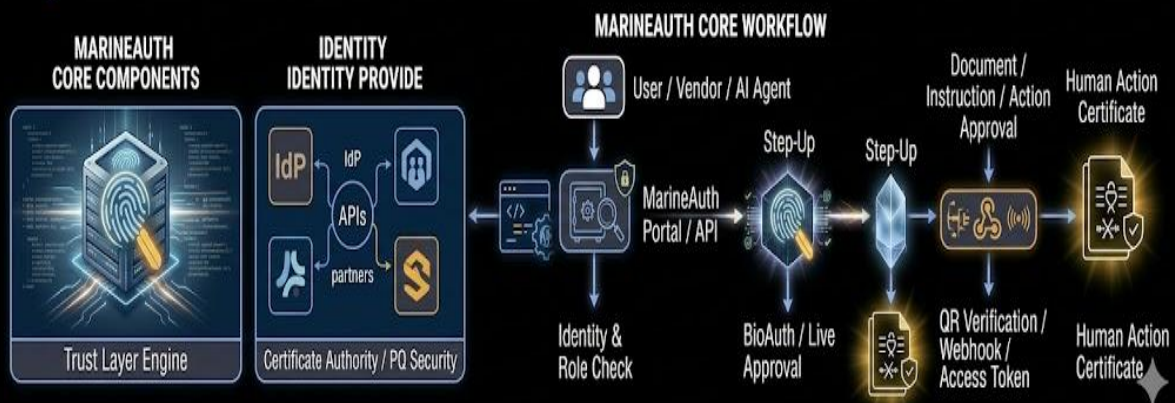
### **Value**

MarineAuth AI Agent Control lets maritime organisations use AI safely without giving AI unchecked authority over critical operations.

## **5. How MarineAuth Works Technically**



# MARINEAUTH: THE API-FIRST TRUST LAYER



## Core components

### 1. MarineAuth Portal

Used by maritime users to create, approve, sign and verify actions.

### 2. MarineAuth Mobile Approval

Used for biometric approval, live step-up and push confirmation.

### 3. API Gateway

Used by external maritime systems to connect to MarineAuth.

### 4. Identity & Role Registry

Stores verified users, roles, organisations and maritime permissions.

### 5. BioAuth Engine

Verifies the human using SyberKey/OneBioID biometric authentication.

### 6. CPE Policy Engine

Evaluates the action context and decides whether to allow, block, escalate or require step-up.

### 7. FingerSign Engine

Biometrically signs maritime documents and creates QR certificates.

### 8. Verified Instruction Engine

Verifies high-risk maritime communications and email instructions.

### **9. Vendor Access Engine**

Controls JIT remote access and privileged maritime sessions.

### **10. AI Airlock Engine**

Controls AI agent identity, scope and execution approval.

### **11. Human Action Certificate Service**

Generates audit evidence for every critical verified action.

## **6. Human Action Certificate**

The **Human Action Certificate** is one of MarineAuth's most important outputs.

It proves:

- who approved the action;
- their organisation;
- their maritime role;
- what action was approved;
- what document or instruction was involved;
- whether biometric verification occurred;
- whether live biometric step-up occurred;
- whether dual approval occurred;
- when the action occurred;
- from which system or workflow;
- which policy was applied;
- whether the action was approved, rejected or blocked.

### **Example**

For a cargo release, the certificate may show:

Certificate ID: HAC-2026-00091

Action: Cargo Release Approval

Cargo Reference: CONT-ABC123456

Document: Cargo Release Order

Approved By: Authorised Shipping Agent  
Organisation: OceanLine Shipping  
Verification: Live Biometric  
Policy: High Value Cargo Release  
Status: Approved  
Timestamp: 0x xxxx 2026, 10:36 AM  
Document Hash: sha256:9f4a...

This certificate can support:

- internal audit;
- regulator review;
- insurer evidence;
- dispute resolution;
- fraud investigation;
- compliance reporting;
- litigation support.

## 7. Main MarineAuth Use Cases

### Use Case 1: Verified Cargo Release

A shipping agent creates a cargo release order. MarineAuth verifies the agent biometrically, checks authority, signs the document and provides a QR verification certificate. The terminal verifies before releasing cargo.

### Use Case 2: Verified Bill of Lading

A bill of lading is signed through MarineAuth. The recipient verifies the signer, organisation, document hash and certificate. Altered copies fail verification.

### Use Case 3: Verified Bank Detail Change

A freight payment bank-detail change is sent through MarineAuth Verified Instructions. The recipient confirms that the sender was biometrically verified before acting.

### Use Case 4: Vendor Access to Vessel Systems

An engine vendor requests remote access. MarineAuth verifies the vendor and requires chief engineer approval before issuing time-bound access.

### Use Case 5: Port Terminal Override

A terminal operator attempts to override a cargo hold. MarineAuth requires supervisor biometric approval before allowing the action.

#### **Use Case 6: AI Route Recommendation**

An AI agent recommends a route change. MarineAuth AI Airlock blocks execution until the captain approves with biometric verification.

#### **Use Case 7: Dangerous Goods Approval**

A dangerous goods movement or port approval requires verified role-based approval and a Human Action Certificate.

#### **Use Case 8: Crew Change Approval**

Crew documentation and approval can be biometrically verified before port clearance or boarding.

## **8. Target Customers**

### **Primary customers**

1. Port authorities
2. Terminal operators
3. Shipping lines
4. Ship managers
5. Freight forwarders
6. Customs brokers
7. Port community system providers
8. Maritime logistics companies
9. Trade finance banks
10. Marine insurers and P&I clubs

### **Secondary customers**

1. Cruise operators
2. Offshore energy operators
3. Vessel maintenance companies
4. Engine/navigation OEMs

5. Maritime cybersecurity vendors
6. Classification and assurance firms
7. Government maritime agencies
8. Border and customs agencies

## 9. Why MarineAuth Is Different

Most maritime cybersecurity tools answer these questions:

- What assets do we have?
- Is there a vulnerability?
- Is there a network anomaly?
- Has an incident occurred?
- Are we compliant?

MarineAuth answers a different and highly practical question:

**Can this person, document, instruction, vendor or AI agent be trusted before this maritime action is allowed?**

That is the gap MarineAuth fills.

### Key differentiators

1. **Biometric identity, not just login credentials**  
MarineAuth verifies the actual authorised human.
2. **Action-level control, not only access control**  
A person may log in, but high-risk actions still require verification.
3. **Document trust built in**  
MarineAuth can biometrically sign and verify maritime documents.
4. **Email and instruction verification**  
MarineAuth protects against fake or compromised maritime instructions.
5. **Vendor access governance**  
Remote maintenance becomes time-bound, approved and auditable.
6. **AI governance built for maritime operations**  
AI agents can be identified, scoped and blocked from execution without human approval.



## 7. **Human Action Certificate**

Every critical action can produce evidence.

## 8. **Complementary, not disruptive**

MarineAuth can integrate with existing maritime cybersecurity, port, logistics and identity systems.

# 10. Product Scope

## Workflow 1: Cargo Release Verification

- create cargo release request;
- verify user role;
- require BioAuth;
- FingerSign release document;
- generate QR certificate;
- terminal verifies release;
- Human Action Certificate issued.

## Workflow 2: Maritime Document Signing

- upload document;
- hash document;
- biometric signing;
- QR verification certificate;
- document verification portal;
- tamper detection.

## Workflow 3: Verified Maritime Instruction

- create high-risk instruction;
- classify risk;
- require BioAuth;
- send verified instruction;
- recipient verifies certificate;
- Human Action Certificate issued.

#### **Workflow 4: Vendor / AI Approval**

- vendor or AI requests access/action;
- CPE policy evaluation;
- authorised human approval;
- time-bound token or execution release;
- Human Action Certificate issued.

### **11. Integration Strategy**

MarineAuth can integrate through APIs, webhooks and QR verification.

#### **Potential integrations**

- Microsoft Entra ID;
- Okta;
- CyberArk;
- ARCON;
- BeyondTrust;
- Marlink remote access/connectivity;
- terminal operating systems;
- port community systems;
- shipping line portals;
- freight forwarding platforms;
- email systems;
- document management platforms;
- SIEM/SOC systems;
- maritime AI systems.

#### **Integration outputs**

MarineAuth can return:

- verified identity result;
- approval token;

- signed document certificate;
- cargo release verification result;
- access token;
- AI Airlock decision;
- Human Action Certificate;
- audit event webhook.

## **13. Commercial Packaging**

### **Package 1: MarineAuth Cargo Release**

For ports, terminals, shipping agents and logistics companies.

Includes:

- verified release order;
- biometric signer;
- QR certificate;
- terminal verification;
- Human Action Certificate.

### **Package 2: MarineAuth Document & Instruction Trust**

For freight forwarders, shipping lines, banks and insurers.

Includes:

- FingerSign Maritime;
- Verified Instructions;
- document tamper check;
- verified email/instruction trail;
- certificate portal.

### **Package 3: MarineAuth Secure Maritime Access**

For ship managers, port authorities and vendors.

Includes:

- BioAuth;
- vendor access approval;
- Bio-PAM;
- CPE policy enforcement;
- privileged command approval;
- audit reporting.

### **Package 4: MarineAuth AI Control**

For advanced ports, fleets and AI-enabled maritime operators.

Includes:

- AI Agent Identity;
- AI sponsor binding;
- AI Airlock;
- verified execution approval;
- AI action certificates.

## **14. Commercial Benefits**

### **For ports and terminals**

- reduce cargo release fraud;
- control terminal overrides;
- verify contractors and vendors;
- strengthen audit and compliance;
- protect critical port operations.

### **For shipping lines and ship managers**

- secure vessel access;
- verify captain/chief engineer approvals;
- control remote maintenance;
- protect cargo documents;
- reduce impersonation risk.

### **For freight forwarders and logistics providers**

- verify release instructions;
- prevent fake payment changes;
- create trusted document workflows;
- reduce email fraud.

### **For banks and insurers**

- strengthen trade document trust;
- reduce bill of lading fraud exposure;
- support claims and dispute evidence;
- improve transaction assurance.

### **For AI-enabled maritime operators**

- prevent uncontrolled AI execution;
- identify AI agents;
- bind AI agents to human sponsors;
- create AI action audit trails.

## **15. Example Customer Story**

A shipping agent needs to release high-value cargo at a container terminal.

Without MarineAuth, the terminal may rely on an emailed release order, a PDF document or ordinary portal login. If the email or account is compromised, cargo may be released fraudulently.

With MarineAuth:

1. The shipping agent creates the cargo release request.
2. MarineAuth verifies the agent's identity and role.
3. The agent completes live BioAuth.
4. The cargo release order is FingerSigned.
5. A QR verification certificate is generated.
6. The terminal scans or checks the certificate.
7. MarineAuth confirms the release is valid.
8. Cargo is released.
9. A Human Action Certificate is issued.

The result is a verified, auditable, fraud-resistant cargo release workflow.

## 16. Final Product Statement

**MarineAuth is the maritime vertical application of SyberKey/OneBioID's patented trust infrastructure.**

It converts maritime cybersecurity from a purely defensive activity into a verified-action control system. It protects not only systems, but the real-world decisions that move cargo, approve documents, grant access, release payments, authorise vendors and govern AI agents.

**MarineAuth verifies the human, document, instruction, vendor or AI agent behind every critical maritime action — before cargo, access, payment or execution is released**