Stichting Innovatieve Waterwegen

Koppelvlak documentatie

Inhoud

Introductie

De Stichting Innovatieve Waterwegen (STIW) vertegenwoordigt een initiatief dat zich richt op de modernisering en verbetering van de digitale infrastructuur en diensten in de maritieme sector. Door innovatie en technologische vooruitgang aan te wenden, streeft STIW ernaar om de digitale efficiëntie en veiligheid van scheepvaartverkeer en havenfaciliteiten te vergroten. In dit licht speelt de invoering van een geavanceerd toegang en identiteitsbeheersysteem een cruciale rol in het realiseren van STIW's visie om een gestroomlijnde, interoperabele en veilige omgeving voor gebruikers en aanbieders te scheppen.

Doel van STIW

STIW's kernmissie is om door middel van samenwerking en de implementatie van slimme technologieën een geïntegreerd koppelvlak te bieden dat het beheer van digitale informatie transformeert. Het koppelvlak faciliteert naadloze communicatie en transacties tussen schippers, havenbeheerders, serviceproviders, overheidsinstanties etc.

Samenvatting van Componenten

Hardware	Omvat alle fysieke componenten die essentieel zijn voor bijvoorbeeld walstroomvoorzieningen en andere maritieme diensten.
Software voor Havenbeheer	Systemen gebruikt door havens, gemeenten en overheden voor het beheren van operaties.
Software voor Onderhoud en Beheer	Bevat hulpmiddelen voor het beheren en onderhouden van infrastructuur.
API Protocol (OFP) en Interface (OFI)	Deze protocollen standaardiseren de communicatie tussen verschillende systemen en diensten, zorgen voor interoperabiliteit en het verminderen van 'vendor lock-in'.
Datasets	De verschillende datasets bevatten informatie zoals transactiegegevens, gebruikersidentiteiten, servicegebruik, openbare data van derden, storingen en locatiegegevens, die van cruciaal belang zijn voor operationele en analytische doeleinden.
Facturatiepartij en Netbeheerder	Deze entiteiten zijn verantwoordelijk voor de economische transacties en het netwerkbeheer binnen het koppelvlak.
Apps en Eindgebruikers	Omvatten de mobiele en webtoepassingen die worden gebruikt door schippers en andere eindgebruikers voor interactie met de services van het koppelvlak.

Hardware

De STIW zet zich in voor het stroomlijnen en standaardiseren van de interactie tussen de hardware van verschillende leveranciers en het overkoepelende digitale koppelvlak voor waterwegbeheer. STIW voorziet niet zelf in de hardware, maar speelt een cruciale rol in het definiëren van de specificaties en protocollen waaraan deze hardware moet voldoen om compatibel te zijn met het STIW-koppelvlak.

Standaardisatie van Hardwareinterfaces:

STIW stelt strikte richtlijnen en normen op waaraan walstroomkasten en andere havenfaciliteiten moeten voldoen. Dit zorgt ervoor dat, ongeacht de hardwareleverancier, alle apparatuur naadloos kan integreren met het STIW-koppelvlak.

Door het vaststellen van standaardinterfaces en communicatieprotocollen verzekert STIW dat alle aangesloten apparatuur de nodige gegevens kan leveren in een formaat dat door het systeem begrepen en verwerkt kan worden.

Communicatieprotocollen (OFP):

Het Openbaar Faciliteiten Protocol (OFP) is het door STIW ontwikkelde protocol dat beschrijft hoe hardware-informatie moet worden uitgewisseld tussen de fysieke infrastructuur en de digitale systemen.

OFP dient als een uniforme taal voor apparatuur van verschillende fabrikanten, waardoor gegevensconsistentie en -integratie worden gewaarborgd.

Verzameling van Operationele Data (Dataset 1):

Hoewel de hardware zelf door externe leveranciers wordt verzorgd, is het aan STIW om ervoor te zorgen dat de gegevens van deze hardware (zoals energieverbruik, gebruiksduur en eventuele diagnostische informatie) correct worden verzameld in Dataset 1.

Deze gestandaardiseerde dataverzameling stelt STIW in staat om accurate en real-time gegevensanalyse te verrichten, waardoor het digitale beheer van havenfaciliteiten efficiënter wordt.

Autorisatie en Beveiliging:

De richtlijnen van STIW omvatten ook beveiligingsprotocollen en autorisatiemethoden om ervoor te zorgen dat enkel geautoriseerde gebruikers toegang krijgen tot de diensten.

De hardware moet geavanceerde beveiligingsmechanismen ondersteunen die door STIW zijn gespecificeerd, zoals encryptie en veilige authenticatieprocessen.

STIW neemt de verantwoordelijkheid voor het faciliteren van een koppelvlak waarin hardware van verschillende leveranciers naadloos kan samenwerken door een gemeenschappelijk raamwerk en set aan communicatie-eisen aan te bieden. Dit maakt het mogelijk voor de hardwarecomponenten om geïntegreerd te worden in het bredere digitale beheersysteem dat STIW voor ogen heeft, zonder dat de stichting zelf de fysieke apparaten hoeft te leveren of te onderhouden. Dit model stelt STIW in staat om een centrale rol te spelen in het innovatieproces, terwijl het toch de flexibiliteit en diversiteit van apparatuur van meerdere leveranciers behoudt.

Havenmanagement Software

De STIW stelt een koppelvlak ter beschikking voor havenmanagement software, zonder zelf software te leveren. Dit koppelvlak faciliteert een uniforme aanpak voor de integratie van diverse

softwareoplossingen aangeboden door verschillende providers, met als doel de efficiëntie, veiligheid en interoperabiliteit binnen het maritieme beheer te verhogen.

Uniforme Data-uitwisseling:

STIW stelt standaarden vast voor data-uitwisseling die essentieel zijn voor een naadloze communicatie tussen havenmanagement software en andere systemen binnen de maritieme infrastructuur. Deze standaarden garanderen dat data zoals bijvoorbeeld ligplaatsbezetting en servicegebruik uniform worden gecommuniceerd, onafhankelijk van de softwareleverancier.

Protocol voor Interoperabiliteit:

Door het specificeren van interoperabiliteitsprotocollen, zorgt STIW ervoor dat havenmanagement software van verschillende havens en leveranciers kan “praten” met centrale systemen zoals met operationele systemen en onderhoudsmanagement tools.

Beveiliging en Autorisatie:

Veiligheidsrichtlijnen omvatten voorschriften voor encryptie, data-integriteit en toegangsbeheer. STIW benadrukt het belang van geavanceerde autorisatiemechanismen om te verzekeren dat enkel geautoriseerd personeel en systemen toegang hebben tot gevoelige operationele gegevens.

Integratie met Facturatiesystemen:

Het kader voorziet in richtlijnen voor de integratie met systemen voor facturatie, waarbij havenmanagement software direct kan communiceren met financiële- en registratiesystemen om transacties en dienstgebruik te beheren.

Aanpassingsvermogen en Schaalbaarheid:

De standaarden binnen het koppelvlak zijn ontworpen om flexibel en schaalbaar te zijn, waardoor havenmanagement software kan worden aangepast aan de unieke eisen van elke haven en kan groeien in lijn met veranderende operationele behoeften.

Ondersteuning voor Duurzaamheidsinitiatieven:

STIW moedigt de integratie van softwarefunctionaliteiten aan die duurzaamheidsinitiatieven ondersteunen, zoals het monitoren van milieuprestaties en het beheren van groene energiebronnen.

Real-time Informatie en Analytische Tools:

Het koppelvlak omvat ook de ondersteuning voor real-time dataverzameling en -analyse, waarmee havenoperators direct inzicht krijgen in operationele prestaties en proactief management beslissingen kunnen nemen.

Door het vaststellen van deze richtlijnen en standaarden faciliteert STIW een omgeving waarin havenmanagement software, ongeacht de bron, effectief en efficiënt kan worden geïntegreerd in het bredere maritieme beheernetwerk. Dit stelt havens in staat om te profiteren van geavanceerde technologische oplossingen terwijl ze verzekerd zijn van compatibiliteit en communicatie binnen het koppelvlak.

Software voor Onderhoud en Beheer

De STIW definieert de standaarden en protocollen voor de koppeling van onderhouds- en beheersoftware, die door havens en onderhoudspartijen zelf wordt geleverd. STIW's benadering waarborgt dat, ongeacht de diversiteit aan softwareoplossingen gekozen door individuele havens en onderhoudsbedrijven, er een gestandaardiseerde communicatie en datadeling mogelijk is binnen het koppelvlak.

Standaard Communicatieprotocollen:

STIW specificeert de communicatieprotocollen die essentieel zijn voor het uitwisselen van gegevens tussen de onderhouds- en beheersoftware en andere systemen binnen het koppelvlak. Dit garandeert interoperabiliteit en zorgt ervoor dat onderhoudsgegevens naadloos geïntegreerd kunnen worden met operationele en logistieke processen.

Interoperabiliteit en Data Uitwisseling:

De door STIW voorgeschreven standaarden omvatten richtlijnen voor data-uitwisseling, waaronder formaten en structuren die ervoor zorgen dat informatie over onderhoudsactiviteiten en -status beschikbaar en begrijpelijk is voor alle relevante partijen, ongeacht het specifieke softwareplatform.

Integratie met Externe Systemen:

Richtlijnen voor de integratie met externe systemen, zoals specifieke operationele software van havens, stellen havens en onderhoudspartijen in staat om hun eigen softwareoplossingen te gebruiken terwijl ze toch verbonden blijven met het koppelvlak.

Veiligheids- en Beveiligingsstandaarden:

Veiligheid en beveiliging zijn cruciale overwegingen. STIW stelt strenge beveiligingsnormen vast voor de onderhouds- en beheersoftware om de bescherming van gevoelige gegevens te waarborgen. Dit omvat encryptie, toegangscontrole en andere cybersecuritypraktijken.

Autorisatiemechanismen:

Voor de toegang tot en het beheer van onderhouds- en beheersoftware definieert STIW autorisatiemechanismen. Deze mechanismen verzekeren dat alleen geautoriseerd personeel toegang heeft tot de softwarefuncties, wat essentieel is voor het behoud van de integriteit en veiligheid van de systemen.

Ondersteuning voor Toekomstige Technologieën:

De standaarden zijn ontworpen om flexibel en toekomstbestendig te zijn, met ondersteuning voor de integratie van nieuwe technologieën en methodologieën die de efficiëntie en effectiviteit van onderhoudswerkzaamheden kunnen verbeteren.

STIW's benadering zorgt ervoor dat havens en onderhoudspartijen de vrijheid hebben om software te kiezen die het beste past bij hun specifieke behoeften, terwijl ze toch profiteren van het koppelvlak dat gestandaardiseerde data-uitwisseling en communicatie bevordert. Dit resulteert in een meer verbonden, efficiënte en veilige maritieme sector.

API Protocol

Het API (Application Programming Interface) Protocol binnen het kader van de STIW vormt de ruggengraat van de digitale communicatie tussen verschillende software- en hardwarecomponenten binnen het koppelvlak. STIW stelt een reeks van standaarden en specificaties op voor dit protocol om te verzekeren dat er een gestroomlijnde, veilige en efficiënte uitwisseling van gegevens plaatsvindt, onafhankelijk van de specifieke technologieën of platforms die door de havens en hun partners worden gebruikt.

Gestandaardiseerde Dataformaten:

STIW specificeert uniforme dataformaten voor het uitwisselen van informatie, zoals JSON of XML, om te verzekeren dat gegevens gemakkelijk geïnterpreteerd en verwerkt kunnen worden door verschillende systemen.

Beveiligingsprotocollen:

Het API Protocol omvat strenge beveiligingsprotocollen zoals HTTPS, OAuth voor autorisatie, en JWT (JSON Web Tokens) voor veilige data-overdracht. Deze maatregelen zorgen voor de bescherming van gevoelige informatie tijdens de overdracht tussen systemen.

Interoperabiliteit:

Door het definiëren van duidelijke en consistente API-endpoints en -methoden, faciliteert STIW de interoperabiliteit tussen systemen van verschillende leveranciers. Dit zorgt voor een soepele samenwerking tussen bijvoorbeeld havenmanagement software, onderhouds- en beheersystemen, en hardwarecomponenten.

Versiebeheer en Compatibiliteit:

STIW voorziet in richtlijnen voor API-versiebeheer om de continuïteit en compatibiliteit van systemen te waarborgen, zelfs wanneer upgrades of wijzigingen worden doorgevoerd. Dit omvat het onderhouden van backwards-compatibiliteit en het duidelijk communiceren van wijzigingen aan alle betrokken partijen.

Foutafhandeling en Feedbackloops:

Het protocol bevat gedetailleerde specificaties voor foutafhandeling en feedbackloops, waardoor systemen adequaat kunnen reageren op fouten of afwijkingen in de data-uitwisseling, en zo de robuustheid van het koppelvlak verhogen.

Real-time Data-uitwisseling en-Verwerking:

Richtlijnen voor real-time data-uitwisseling stellen havens en gerelateerde entiteiten in staat om direct te reageren op operationele gebeurtenissen, waardoor de efficiëntie en reactiesnelheid van de beheerder worden verhoogd.

Documentatie en Ontwikkelaarsondersteuning:

STIW zorgt voor uitgebreide documentatie van het API Protocol, inclusief technische specificaties, gebruiksinstructies en best practices. Dit bevordert de adoptie en implementatie van het protocol door softwareontwikkelaars en systeemintegratoren.

Door deze richtlijnen en standaarden te hanteren, stimuleert STIW de creatie van een flexibel, schaalbaar en veilig digitaal koppelvlak. Dit koppelvlak ondersteunt naadloze communicatie en data-uitwisseling tussen een breed scala aan maritieme en havengebonden activiteiten, waardoor de weg vrijgemaakt wordt voor innovatie en verbeterde operationele efficiëntie binnen de maritieme sector.

API Eindpunten:

Voor de implementatie van de datasets binnen het STIW-koppelvlak, is het essentieel om duidelijke API-eindpunten te definiëren voor elke dataset. Hieronder volgen enkele voorbeelden van hoe deze eindpunten kunnen worden gestructureerd:

Voorziening Detectie:

Endpoint: /api/v1/facility/detect

Method: POST

Request Body:

```
{
  "facilityID": "string",
  "facilityType": "string",
  "status": "string"
}
```

Response:

```
{
  "status": "success",
  "message": "Facility detected successfully"
}
```

Transactiebeheer:

Endpoint: /api/v1/transaction/start

Method: POST

Request Body:

```
{
  "userID": "string",
  "facilityID": "string",
  "facilityType": "string",
  "timestamp": "string"
}
```

Response:

```
{
  "status": "success",
  "message": "Transaction started successfully"
```

}

Energiemeting en-verbruik:

Endpoint: /api/v1/energy/consumption

Method: GET

Parameters:

facilityID

timestamp

Response:

```
{
  "facilityID": "string",
  "facilityType": "string",
  "unitsConsumed": "number",
  "timestamp": "string"
}
```

Authenticatie- en Autorisatiemechanismen:

OAuth 2.0:

Authorization Endpoint: /oauth2/authorize

Token Endpoint: /oauth2/token

Scopes: Define specific scopes for read and write access to different datasets, e.g., facility:read, facility:write, transaction:read, transaction:write.

JWT (JSON Web Tokens):

Usage: Issue JWTs to authenticated users, which include claims about the user's identity and permissions.

Header:

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Payload:

```
{
  "sub": "userID",
  "iat": 1516239022,
```

"exp": 1516239022,

"scope": "facility:read facility:write"

}

Signature: HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), secret)

Dataformaten:

JSON:

Example:

{

"facilityID": "12345",

"facilityType": "charger",

"status": "active"

}

XML:

Example:

<Facility>

<FacilityID>12345</FacilityID>

<FacilityType>charger</FacilityType>

<Status>active</Status>

</Facility>

Integratie en Interoperabiliteit

Integratie met Bestaande Systemen:

API Gateway:

Function: Acts as an entry point for all API requests, managing traffic, and ensuring security.

Features: Rate limiting, IP whitelisting, API key management, logging and monitoring.

Webhooks:

Usage: For real-time updates, e.g., when a facility's status changes or a transaction is started.

Endpoint Registration: Clients can register their endpoints to receive webhook notifications.

Example Payload:

```
{
  "event": "facility_status_update",
  "data": {
    "facilityID": "12345",
    "newStatus": "inactive",
    "timestamp": "2024-06-20T12:34:56Z"
  }
}
```

Interoperabiliteit met Andere Platforms:

Standard Protocols:

RESTful APIs: Ensure that all API endpoints conform to REST principles, making it easier for other systems to interact.

GraphQL: Consider using GraphQL for flexible queries and efficient data retrieval.

Data Exchange Standards:

JSON: Primary data format for API responses and requests, due to its wide adoption and ease of use.

XML: For systems that require XML, ensure all endpoints can also return XML formatted data.

Security Standards:

TLS (Transport Layer Security): Ensure all data exchanges are encrypted using TLS to protect sensitive information.

IAM (Identity and Access Management): Implement robust IAM policies to control access to different datasets and endpoints.

Middleware for Legacy Systems:

Adapters: Develop adapters to translate between modern APIs and legacy systems that may use older protocols like SOAP.

ETL (Extract, Transform, Load): Use ETL tools to integrate and sync data between STIW and other systems, ensuring data consistency and accuracy.

Autorisatiemodel

Het autorisatiemodel onder de vleugels van de STIW speelt een cruciale rol in het waarborgen van de beveiliging en integriteit van het koppelvlak. Dit model omvat de procedures en technologieën die gebruikt worden om te bepalen of en hoe gebruikers toegang krijgen tot verschillende onderdelen van het systeem, van data tot functionaliteiten. STIW ontwikkelt een raamwerk van standaarden en richtlijnen die de basis vormen voor een veilige en controleerbare toegang tot informatie en systemen.

Gebruikersauthenticatie:

Een stevig fundament van het autorisatiemodel is een robuust systeem voor gebruikersauthenticatie, dat identiteiten verifieert voordat toegang wordt verleend. Methoden zoals tweefactorauthenticatie (2FA), sterke wachtwoordbeleid en biometrische verificatie zijn voorbeelden van de aanbevelingen door STIW.

Rol gebaseerde Toegangscontrole (RBAC):

STIW promoot het gebruik van rol gebaseerde toegangscontrole waarbij toegangsrechten worden toegekend op basis van de rol van een gebruiker binnen de organisatie. Dit zorgt voor een granulaire controle over wie toegang heeft tot wat, en faciliteert een minimale toegangsrechtenprincipe (principle of least privilege).

OAuth 2.0 en Tokens:

Voor het beheren van autorisaties tussen verschillende systemen, stelt STIW voor om standaardprotocollen zoals OAuth 2.0 te gebruiken. Dit protocol maakt gebruik van tokens die beperkte toegangsrechten verlenen aan applicaties zonder dat de gebruikersgegevens worden onthuld.

API Sleutelbeheer:

API sleutels worden gebruikt om de toegang tot bepaalde functies en gegevens via het API protocol te reguleren. STIW stelt standaarden vast voor het beheer van deze sleutels, waaronder de uitgifte, rotatie en intrekking van sleutels om veiligheidsrisico's te minimaliseren.

Audit Trails en Monitoring:

Het autorisatiemodel voorziet in uitgebreide logging en monitoring van toegangs- en activiteitpogingen. Dit stelt beheerders in staat om ongeautoriseerde toegangspogingen te detecteren en te reageren op potentiële veiligheidsincidenten.

Data Encryptie:

STIW beveelt aan dat alle gegevens, zowel in rust als in transit, versleuteld moeten zijn om de vertrouwelijkheid en integriteit van informatie te beschermen. Dit omvat het gebruik van industriestandaard encryptieprotocollen zoals TLS (min. 3.0) voor gegevens die over het internet worden verzonden.

Fijnmazige Autorisatie:

Voor geavanceerde controle stelt STIW voor om fijnmazige autorisatiemechanismen te implementeren die gedetailleerde toegangsbeleid ondersteunen, gebaseerd op gebruikersattributen, context en andere relevante criteria.

Door het vaststellen van deze richtlijnen zorgt STIW ervoor dat alle betrokken partijen binnen het koppelvlak een veilige en gestructureerde benadering kunnen hanteren voor autorisatie en

toegangsbeheer. Dit bevordert een veilige omgeving waarin gegevens en systemen beschermd zijn tegen ongeautoriseerde toegang, terwijl legitieme gebruikers de toegang krijgen die ze nodig hebben om hun werk effectief uit te voeren.

Scenario: Nieuwe Klant Registratie en Autorisatie

Registratie van de Nieuwe Klant:

Gebruiker: Bob opent de app en selecteert de optie om een nieuw account aan te maken.

Actie: Bob vult het registratieformulier in de app in met zijn persoonlijke gegevens en gaat akkoord met de voorwaarden. De app-aanbieder slaat Bobs gegevens veilig op in zijn eigen database.

Aanmaken van Authenticatie Credentials:

Actie: Na de registratie genereert de app-aanbieder unieke inloggegevens voor Bob en vraagt Bob om deze te gebruiken bij het aanmelden.

Veiligheid: De app-aanbieder zorgt ervoor dat alle communicatie en opgeslagen gegevens versleuteld zijn om Bobs privacy te beschermen.

Centrale Autorisatie en Token Uitgifte:

Autorisatie Verzoek: Wanneer Bob de app gebruikt om toegang te krijgen tot diensten zoals het activeren van walstroom, stuurt de app een autorisatieverzoek naar de centrale autorisatieserver van STIW.

Token Uitgifte: De centrale autorisatieserver verifieert Bobs credentials (via de app-aanbieder) en geeft een toegangstoken uit. Dit token bevestigt dat Bob geautoriseerd is om de gevraagde dienst te gebruiken zonder dat zijn persoonlijke gegevens bij STIW worden opgeslagen.

Gebruik van de Dienst:

Actie: Met het toegangstoken kan Bob nu de walstroomkast activeren. De token valideert Bobs toegangsrechten voor de activering van de kast via de app.

Transactiegegevens: Gebruiksgegevens zoals tijd en energieverbruik worden anoniem of met een unieke, niet-persoonlijk identificeerbare referentie geregistreerd voor facturatiedoeleinden.

Facturatie en Privacy:

Facturatie: De app stuurt de anonieme of pseudonieme transactiegegevens naar de facturatiepartij voor het genereren van een factuur. Bob ontvangt deze factuur via de app of e-mail.

Gegevensopslag: De app-aanbieder beheert Bobs persoonlijke en facturatiegegevens, terwijl STIW ervoor zorgt dat de operationele data losgekoppeld blijven van persoonlijke identificatie, in lijn met privacy reguleringen.

Veiligheid en Centrale Autorisatie

Dit model zorgt ervoor dat, ondanks dat STIW geen persoonlijke gebruikersgegevens opslaat, er een efficiënte en veilige methode is voor het verlenen van toegang en autorisatie. Het maakt gebruik van centrale autorisatie voor diensttoegang terwijl de privacy van de gebruiker wordt beschermd en de verantwoordelijkheid voor gegevensopslag bij de app-aanbieder ligt.

Integratie van Federale Gegevens in het Autorisatieproces

Verificatie bij Eerste Registratie:

Actie: Tijdens het registratieproces kan de app van Bob een verificatieverzoek indienen bij een federale gegevensdienst om Bobs identiteit en de status te controleren. Dit zorgt voor een extra laag van vertrouwen en veiligheid.

Privacy: Alle verzoeken aan federale databases worden uitgevoerd met strikte naleving van privacywetgeving en met expliciete toestemming van Bob.

Aanvulling:

Technische Implementatie: Bij de eerste registratie stuurt de app een verzoek naar een API van de federale gegevensdienst, waarbij gebruik wordt gemaakt van OAuth 2.0 voor veilige toegang. De gegevensdienst retourneert een token dat bevestigt dat Bob geverifieerd is. Dit token wordt opgeslagen in de beveiligde omgeving van de app.

Gebruik van Federale Gegevens voor Autorisatie:

Autorisatie Verzoek: Wanneer Bob toegang probeert te krijgen tot bepaalde diensten via de app, kan de centrale autorisatieserver van STIW federale gegevens gebruiken als onderdeel van het autorisatieproces. Bijvoorbeeld, het kan controleren of Bobs schip momenteel een geldige milieucertificering heeft voordat het toegang geeft tot milieugevoelige diensten.

Dynamische Toegangscontrole: Door federale gegevens te integreren, kan STIW dynamische toegangscontrole implementeren, waarbij de toegangsrechten van Bob automatisch worden aangepast op basis van de actuele status van zijn certificaten en vergunningen.

Aanvulling:

Technische Implementatie: De autorisatieserver van STIW maakt gebruik van federatieve identiteitsbeheerprotocollen zoals SAML (Security Assertion Markup Language) om toegang te verkrijgen tot de federale gegevensdienst. Een XML-gebaseerd SAML-assertion wordt gebruikt om Bobs milieucertificeringsstatus te valideren voordat toegang wordt verleend.

Continue Verificatie:

Periodieke Checks: De app kan periodiek federale gegevens raadplegen om ervoor te zorgen dat Bobs gegevens up-to-date zijn. Dit helpt bij het handhaven van een hoog veiligheidsniveau en zorgt ervoor dat enkel gekwalificeerde gebruikers toegang hebben tot bepaalde diensten.

Automatische Updates: Bij wijzigingen in Bobs status of certificeringen, kan de app automatisch zijn toegangsrechten bijwerken, waardoor het risico op ongeautoriseerde toegang verder wordt verkleind.

Aanvulling:

Technische Implementatie: Periodieke checks worden uitgevoerd door middel van een cron job die op de achtergrond draait en op regelmatige tijdsintervallen verzoeken stuurt naar de federale gegevensdienst. Webhooks kunnen ook worden gebruikt om real-time updates te ontvangen van de federale gegevensdienst bij wijzigingen in de certificeringsstatus.

Facturatie en Compliance Reporting:

Transparantie: Door integratie met federale gegevens kunnen facturatieprocessen en compliance reporting verder worden geautomatiseerd en gestroomlijnd. Dit zorgt voor een hogere transparantie en vereenvoudigt het naleven van regelgeving voor zowel Bob als de havenbeheerders.

Aanvulling:

Technische Implementatie: De facturatie- en compliance-systemen van STIW kunnen via RESTful API's communiceren met federale gegevensdiensten om de nodige data op te halen voor rapportage en facturatie. Een beveiligde datawarehouse kan worden gebruikt om de verzamelde gegevens te analyseren en rapportages te genereren.

Voordelen van het Gebruik van Federale Gegevens

Verbeterde Veiligheid en Vertrouwen: Door federale gegevens te integreren, kan het systeem de identiteit en kwalificaties van gebruikers nauwkeuriger verifiëren, wat leidt tot een veiligere gebruiksomgeving.

Dynamische Autorisatie: De mogelijkheid om toegangsrechten automatisch aan te passen op basis van de actuele status van gebruikers verbetert de flexibiliteit en responsiviteit van het autorisatiemodel.

Efficiëntie in Compliance: Automatisering van compliance-gerelateerde processen vermindert de administratieve last voor gebruikers en havenbeheerders, waardoor ze zich kunnen concentreren op hun kernactiviteiten.

Aanvulling:

Technische Implementatie: Door gebruik te maken van federatieve identiteitstandaarden zoals OAuth 2.0, SAML en OpenID Connect, kan STIW een robuust en schaalbaar autorisatiemodel opzetten. Dit model kan naadloos federale gegevens integreren en real-time toegangsbeheer mogelijk maken.

Door federale gegevens slim te integreren binnen het autorisatiemodel, faciliteert STIW een meer geïntegreerde, responsieve en veilige digitale infrastructuur die bijdraagt aan een soepele en compliant operatie van maritieme activiteiten binnen het koppelvlak.

Beschikbaarheid en Toegang:

Actie: STIW faciliteert toegang tot open data sets via gestandaardiseerde API's, waarbij zowel de integriteit als de actualiteit van de gegevens gewaarborgd is. Dit stelt alle betrokken partijen in staat om relevante open data gemakkelijk te raadplegen en te integreren in hun operationele processen.

Gebruik van Open Data voor Besluitvorming:

Gebruikers en Havenbeheerders: Door open data te integreren, kunnen gebruikers zoals Bob en havenbeheerders zoals Alice actuele informatie gebruiken om geïnformeerde beslissingen te nemen. Bijvoorbeeld, Alice kan waterstanden gebruiken voor het plannen van onderhoudswerkzaamheden, terwijl Bob weerinformatie kan raadplegen om zijn reisplanning te optimaliseren.

Verbeterde Dienstverlening:

App-aanbieders: App-aanbieders kunnen open data integreren om hun dienstverlening te verbeteren, zoals het aanbieden van gepersonaliseerde routeadviezen of veiligheidswaarschuwingen op basis van actuele milieu- en verkeersgegevens.

Compliance en Milieubewustzijn:

Rapportage: Open data kan worden gebruikt voor het genereren van compliance rapporten en voor het bevorderen van milieubewustzijn. Havens kunnen bijvoorbeeld hun CO2-voetafdruk rapporteren en initiatieven voor duurzaamheid promoten op basis van geïntegreerde milieu-informatie.

Beveiliging en Autorisatie voor Open Data:

Autorisatiemodel: Hoewel open data vrij toegankelijk is, zorgt STIW voor de implementatie van beveiligingsmaatregelen om ongeautoriseerde manipulatie van gegevens te voorkomen. Autorisatieprotocollen zorgen ervoor dat alleen gevalideerde applicaties en gebruikers wijzigingen kunnen aanbrengen of gevoelige datasets kunnen koppelen.

Voordelen van het Gebruik van Open Data

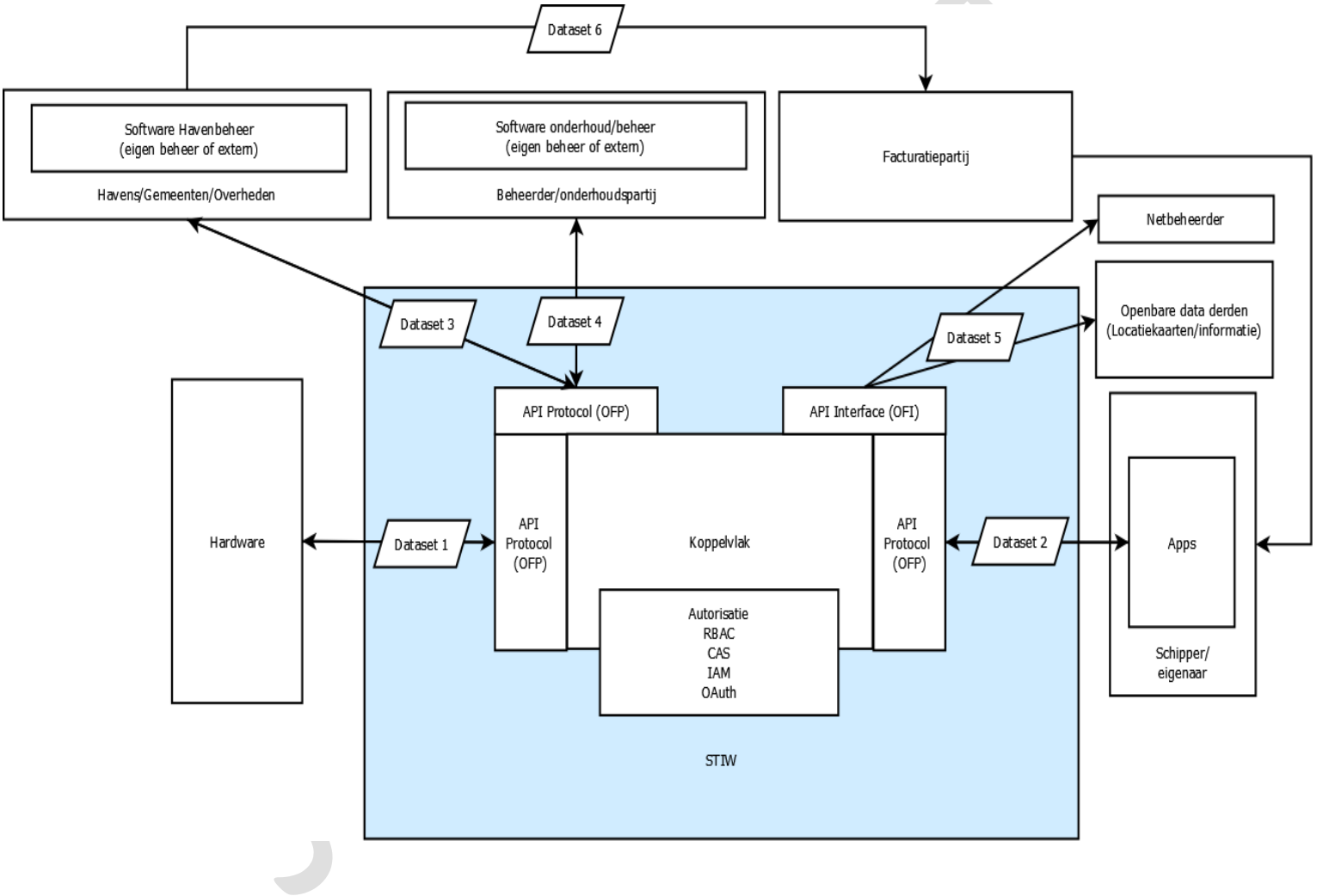
Transparantie en Samenwerking: Open data bevordert een cultuur van transparantie en samenwerking tussen havens, schippers, overheden en de bredere gemeenschap.

Innovatie en Ontwikkeling: Het gemakkelijk beschikbaar maken van open data stimuleert innovatie, bijvoorbeeld door de ontwikkeling van nieuwe apps en diensten die zorgen voor een efficiënt gebruik binnen de maritieme sector.

Data-gedreven Besluitvorming: De integratie van open data ondersteunt data-gedreven besluitvorming, wat leidt tot optimalisatie van operaties en verbetering van de veiligheid en dienstverlening.

Door open data te omarmen en te integreren binnen haar autorisatiemodel en operationele raamwerk, speelt STIW een cruciale rol in het faciliteren van een adaptief, responsief en transparant koppelvlak dat klaar is om de uitdagingen en kansen van de toekomst aan te gaan in de maritieme sector.

Schematisch overzicht



Bijlage 1

Dataset 1 – Hardware

Voorziening Detectie	FacilityDetected: { facilityID, facilityType, status }
Voorziening Detectie	FacilityReleased: { facilityID, facilityType, status }
Voorziening Vergrendeling/ Ontgrendeling	FacilityLockCommand: { facilityID, facilityType, lockStatus }
Voorziening Vergrendeling/ Ontgrendeling	FacilityLockStatus: { facilityID, facilityType, currentLockStatus }
Energiemeting en -verbruik	FacilityConsumptionReport: { facilityID, facilityType, unitsConsumed, timestamp }
Energiemeting en -verbruik	FacilityMeterError: { facilityID, facilityType, errorType }
Transactiebeheer	StartFacilityUsage: { userID, facilityID, facilityType, timestamp }
Transactiebeheer	EndFacilityUsage: { userID, facilityID, facilityType, timestamp, totalUnitsUsed }
Status van de Apparatuur	EquipmentStatus: { aansluitingID, operationalStatus, errorCodes }
Status van de Apparatuur	MaintenanceRequired: { aansluitingID, maintenanceType }
Veiligheids- en Foutmeldingen	FacilitySafetyAlert: { facilityID, facilityType, alertType, timestamp }
Veiligheids- en Foutmeldingen	FacilityFault: { facilityID, facilityType, faultType, reason, timestamp }
UPS Status	UPSStatus: { status, remainingBatteryLife, errorCodes }
Remote Control en Diagnostiek	RemoteOperationRequest: { aansluitingID, operationType }
Remote Control en Diagnostiek	RemoteDiagnosticsReport: { aansluitingID, diagnosticsData }
Geavanceerde Veiligheidscontroles	AdvancedSafetyCheck: { aansluitingID, checkResults }
Netwerkstatus en -kwaliteit	NetworkQualityReport: { locationID, signalStrength, latency }
Status Aardlekschakelaar	EarthLeakageStatus: { aansluitingID, status, lastEventTimestamp }
Status Aardlekschakelaar	EarthLeakageTripped: { aansluitingID, reason, timestamp }
Status Installatieautomaat	CircuitBreakerStatus: { aansluitingID, status, lastEventTimestamp }
Status Installatieautomaat	CircuitBreakerTripped: { aansluitingID, reason, timestamp }
Actueel Gebruik	CurrentFacilityUsage: { facilityID, facilityType, unitsUsed, unitType, timestamp }
Bezettingsstatus	OccupancyStatus: { aansluitingID, isOccupied }
Bezettingsstatus	OccupancyChanged: { aansluitingID, newStatus, timestamp }
Remote Reset en Bediening	RemoteResetRequest: { aansluitingID, deviceType }
Remote Reset en Bediening	RemoteControlCommand: { aansluitingID, command, parameters }
Energiebron en Netwerkstatus	EnergySourceReport: { locationID, energySourceType }
Energiebron en Netwerkstatus	NetworkQualityReport: { locationID, signalStrength, latency }
Weersinvloeden en Smart City Integratie	WeatherConditionReport: { locationID, weatherStatus, potentialImpact }
Weersinvloeden en Smart City Integratie	SmartCityIntegrationData: { cityID, relevantData }
Luik/Deur Open/Dicht Status	AccessDoorStatus: { aansluitingID, doorID, status, timestamp }
Luik/Deur Open/Dicht Status	AccessDoorOpened: { aansluitingID, doorID, timestamp }
Luik/Deur Open/Dicht Status	AccessDoorClosed: { aansluitingID, doorID, timestamp }
Alarmen voor Ongeautoriseerde Toegang	UnauthorizedAccessAlert: { aansluitingID, doorID, timestamp, alertType }
Remote Controle van Toegang	RemoteDoorControl: { aansluitingID, doorID, command, timestamp }

Dataset 2 – Apps eindgebruiker

Voorziening Detectie	FacilityDetected: { facilityID, facilityType, status }
Voorziening Detectie	FacilityReleased: { facilityID, facilityType, status }
Voorziening Vergrendeling/ Ontgrendeling	FacilityLockCommand: { facilityID, facilityType, lockStatus }
Voorziening Vergrendeling/ Ontgrendeling	FacilityLockStatus: { facilityID, facilityType, currentLockStatus }
Energiemeting en -verbruik	FacilityConsumptionReport: { facilityID, facilityType, unitsConsumed, timestamp }
Energiemeting en -verbruik	FacilityMeterError: { facilityID, facilityType, errorType }
Transactiebeheer	StartFacilityUsage: { userID, facilityID, facilityType, timestamp }
Transactiebeheer	EndFacilityUsage: { userID, facilityID, facilityType, timestamp, totalUnitsUsed }
Status van de Apparatuur	EquipmentStatus: { aansluitingID, operationalStatus, errorCodes }
Status van de Apparatuur	MaintenanceRequired: { aansluitingID, maintenanceType }
Veiligheids- en Foutmeldingen	FacilitySafetyAlert: { facilityID, facilityType, alertType, timestamp }
Veiligheids- en Foutmeldingen	FacilityFault: { facilityID, facilityType, faultType, reason, timestamp }
Status Aardlekschakelaar	EarthLeakageStatus: { aansluitingID, status, lastEventTimestamp }
Status Aardlekschakelaar	EarthLeakageTripped: { aansluitingID, reason, timestamp }
Status Installatieautomaat	CircuitBreakerStatus: { aansluitingID, status, lastEventTimestamp }
Status Installatieautomaat	CircuitBreakerTripped: { aansluitingID, reason, timestamp }
Actueel Gebruik	CurrentFacilityUsage: { facilityID, facilityType, unitsUsed, unitType, timestamp }
Bezettingsstatus	OccupancyStatus: { aansluitingID, isOccupied }
Bezettingsstatus	OccupancyChanged: { aansluitingID, newStatus, timestamp }
Remote Reset en Bediening	RemoteResetRequest: { aansluitingID, deviceType }
Remote Reset en Bediening	RemoteControlCommand: { aansluitingID, command, parameters }
Gebruikersinteractie	UserFeedbackRequest: { transactionID }
Gebruikersinteractie	UserFeedbackResponse: { transactionID, feedbackContent }
Dynamische Prijsstelling	FacilityPriceUpdate: { facilityID, facilityType, newPrice, priceUnit, effectiveFrom }

Dataset 3 – Software havenbeheer

Energiemeting en -verbruik	FacilityConsumptionReport: { facilityID, facilityType, unitsConsumed, timestamp }
Energiemeting en -verbruik	FacilityMeterError: { facilityID, facilityType, errorType }
Status van de Apparatuur	EquipmentStatus: { aansluitingID, operationalStatus, errorCodes }
Status van de Apparatuur	MaintenanceRequired: { aansluitingID, maintenanceType }
Actueel Gebruik	CurrentFacilityUsage: { facilityID, facilityType, unitsUsed, unitType, timestamp }
Bezettingsstatus	OccupancyStatus: { aansluitingID, isOccupied }
Bezettingsstatus	OccupancyChanged: { aansluitingID, newStatus, timestamp }
Gebruikersinteractie	UserFeedbackRequest: { transactionID }
Gebruikersinteractie	UserFeedbackResponse: { transactionID, feedbackContent }
Dynamische Prijsstelling	FacilityPriceUpdate: { facilityID, facilityType, newPrice, priceUnit, effectiveFrom }

Dataset 4 – Software beheerder/onderhoud

Status van de Apparatuur	EquipmentStatus: { aansluitingID, operationalStatus, errorCodes }
Status van de Apparatuur	MaintenanceRequired: { aansluitingID, maintenanceType }
Veiligheids- en Foutmeldingen	FacilitySafetyAlert: { facilityID, facilityType, alertType, timestamp }
Veiligheids- en Foutmeldingen	FacilityFault: { facilityID, facilityType, faultType, reason, timestamp }
UPS Status	UPSStatus: { status, remainingBatteryLife, errorCodes }
Remote Control en Diagnostiek	RemoteOperationRequest: { aansluitingID, operationType }
Remote Control en Diagnostiek	RemoteDiagnosticsReport: { aansluitingID, diagnosticsData }
Geavanceerde Veiligheidscontroles	AdvancedSafetyCheck: { aansluitingID, checkResults }
Netwerkstatus en -kwaliteit	NetworkQualityReport: { locationID, signalStrength, latency }
Status Aardlekschakelaar	EarthLeakageStatus: { aansluitingID, status, lastEventTimestamp }
Status Aardlekschakelaar	EarthLeakageTripped: { aansluitingID, reason, timestamp }

Status Installatieautomaat	CircuitBreakerStatus: { aansluitingID, status, lastEventTimestamp }
Status Installatieautomaat	CircuitBreakerTripped: { aansluitingID, reason, timestamp }
Actueel Gebruik	CurrentFacilityUsage: { facilityID, facilityType, unitsUsed, unitType, timestamp }
Bezettingsstatus	OccupancyStatus: { aansluitingID, isOccupied }
Bezettingsstatus	OccupancyChanged: { aansluitingID, newStatus, timestamp }
Remote Reset en Bediening	RemoteResetRequest: { aansluitingID, deviceType }
Remote Reset en Bediening	RemoteControlCommand: { aansluitingID, command, parameters }
Energiebron en Netwerkstatus	EnergySourceReport: { locationID, energySourceType }
Energiebron en Netwerkstatus	NetworkQualityReport: { locationID, signalStrength, latency }
Weersinvloeden en Smart City Integratie	WeatherConditionReport: { locationID, weatherStatus, potentialImpact }
Weersinvloeden en Smart City Integratie	SmartCityIntegrationData: { cityID, relevantData }
Luik/Deur Open/Dicht Status	AccessDoorStatus: { aansluitingID, doorID, status, timestamp }
Luik/Deur Open/Dicht Status	AccessDoorOpened: { aansluitingID, doorID, timestamp }
Luik/Deur Open/Dicht Status	AccessDoorClosed: { aansluitingID, doorID, timestamp }
Alarmen voor Ongeautoriseerde Toegang	UnauthorizedAccessAlert: { aansluitingID, doorID, timestamp, alertType }
Remote Controle van Toegang	RemoteDoorControl: { aansluitingID, doorID, command, timestamp }

Dataset 5 – Open data

Status van de Apparatuur	EquipmentStatus: { aansluitingID, operationalStatus, errorCodes }
Status van de Apparatuur	MaintenanceRequired: { aansluitingID, maintenanceType }
Bezettingsstatus	OccupancyStatus: { aansluitingID, isOccupied }
Bezettingsstatus	OccupancyChanged: { aansluitingID, newStatus, timestamp }
Dynamische Prijsstelling	FacilityPriceUpdate: { facilityID, facilityType, newPrice, priceUnit, effectiveFrom }

Dataset 6 – Software havenbeheer/facturatie (buiten koppelvlak)

Energiemeting en -verbruik	FacilityConsumptionReport: { facilityID, facilityType, unitsConsumed, timestamp }
Dynamische Prijsstelling	FacilityPriceUpdate: { facilityID, facilityType, newPrice, priceUnit, effectiveFrom }