MHHS
PROGRAMME
Industry-led, Elexon facilitated

Deep Dive: Technical

17 August 2022

MHHS-DEL570

Version 0.1 SI Design Assurance Team

Session Overview

Technical

Slido tag:

#MHHSTechnical

Todays presenters:
Robert Golding – MHHS Solution Architect
Kevan Gleeson – MHHS Security Architect

Deep Dive - Technical: Session overview

Approach

- We will use the Design Playback Deep Dives to provide a lower level of detail on the specific topics
- Our Design Subject Matter Experts will take 60-90 minutes to discuss the topics, as well as fielding any questions or comments

Purpose

- Today's session will cover the Data Integration Platform (DIP) in more detail. Focusing on what the DIP is, how Market Participants are meant to interact with it, what resources are available to help with this and the timelines
- We will also respond to any questions, comments or queries you may have

Outcomes

- By the end of today's session, you will have:
    - A better understanding of the Data Integration Platform (DIP)
    - Your question, comments and queries answered or logged to be answered at a later stage

Outputs

- We will issue the slide pack and a link to the recording for this session
- All questions submitted on Slido and asked in person will be logged and the answers transcribed and edited for comprehension
- These will also be issued to all attendees

Slido and Rules of Engagement

- Some questions have been submitted in advance to drive the initial discussion
- Additional questions can be submitted at Slido.com with the code below, or raise your hand on Teams, the facilitator will handle sequencing
- Subject discussions are timeboxed to fifteen minutes to allow breadth of subjects to be discussed

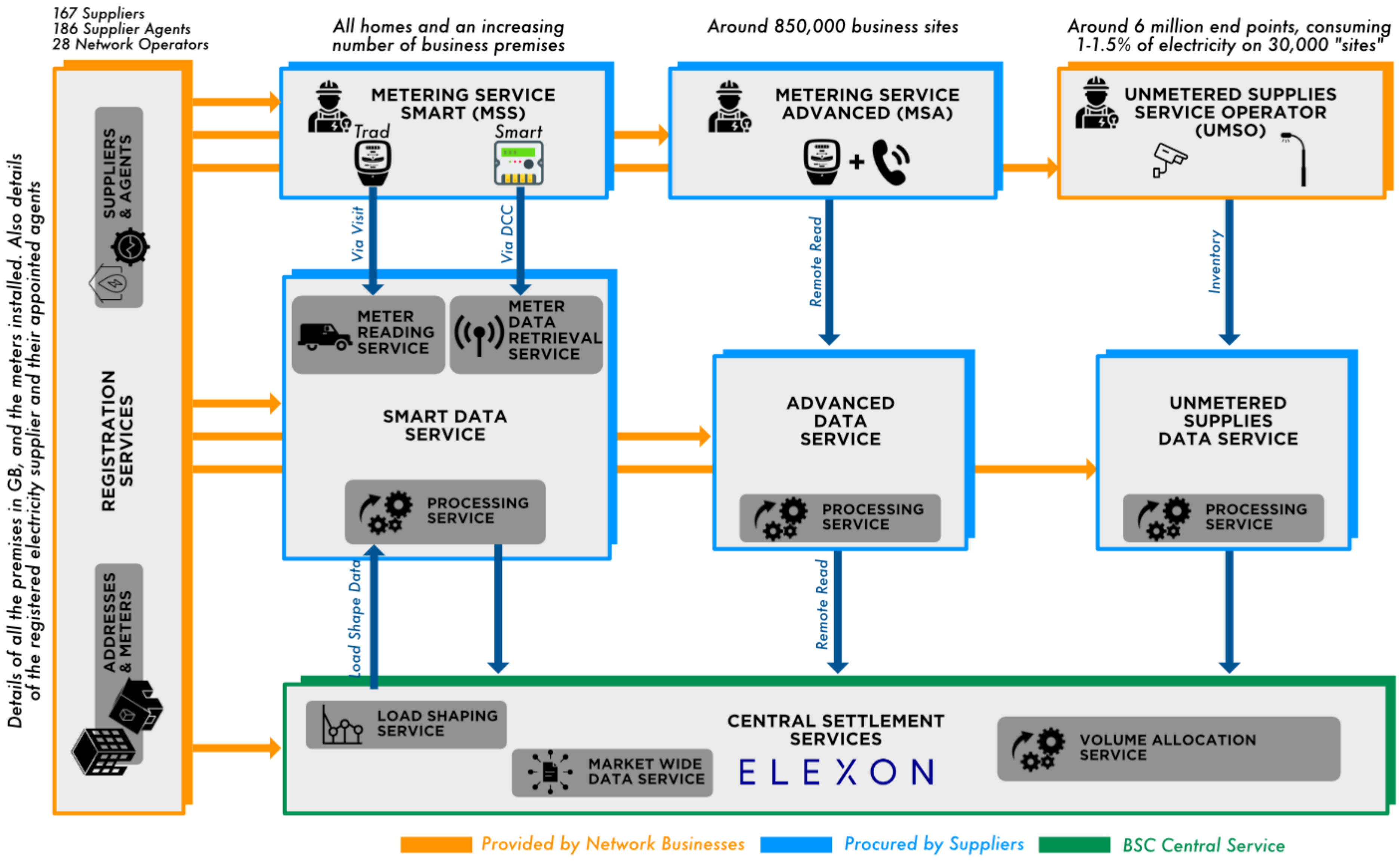
Questions - slido.com #MHHSTechnical

What We’ll Cover Today

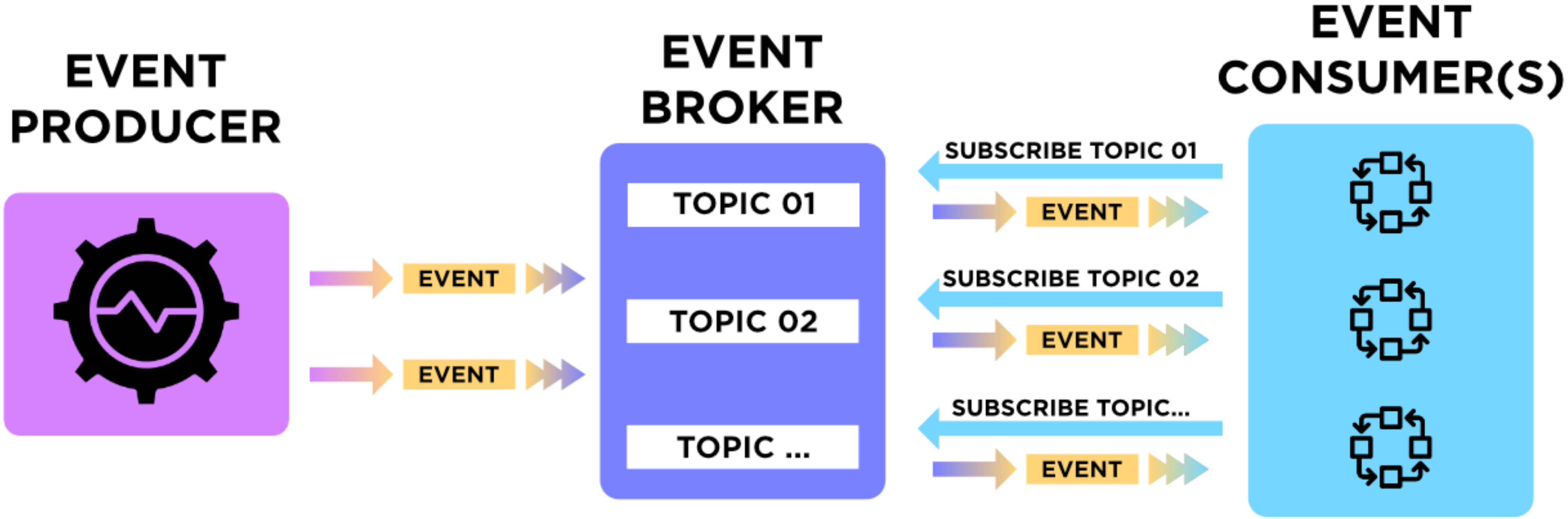
- DIP Overview
- End-to-End Message Exchange
- Security

Deep Dive – Technical: Background #1

Questions - slido.com #MHHSTechnical


167 Suppliers
186 Supplier Agents
28 Network Operators
All homes and an increasing number of business premises
Around 850,000 business sites
Around 6 million end points, consuming 1-1.5% of electricity on 30,000 "sites"
Details of all the premises in GB, and the meters installed. Also details of the registered electricity supplier and their appointed agents
SUPPLIERS & AGENTS
REGISTRATION SERVICES
ADDRESSES & METERS
METERING SERVICE SMART (MSS)
Trad
Smart
Via Visit
Via DCC
METERING SERVICE ADVANCED (MSA)
UNMETERED SUPPLIES SERVICE OPERATOR (UMSO)
Remote Read
Inventory
METER READING SERVICE
METER DATA RETRIEVAL SERVICE
SMART DATA SERVICE
PROCESSING SERVICE
ADVANCED DATA SERVICE
PROCESSING SERVICE
UNMETERED SUPPLIES DATA SERVICE
PROCESSING SERVICE
Load Shape Data
Remote Read
LOAD SHAPING SERVICE
MARKET WIDE DATA SERVICE
CENTRAL SETTLEMENT SERVICES
ELEXON
VOLUME ALLOCATION SERVICE
Provided by Network Businesses
Procured by Suppliers
BSC Central Service

Deep Dive – Technical: Background #2



EVENT PRODUCER

EVENT

EVENT

EVENT BROKER

TOPIC 01

TOPIC 02

TOPIC ...

SUBSCRIBE TOPIC 01

EVENT

SUBSCRIBE TOPIC 02

EVENT

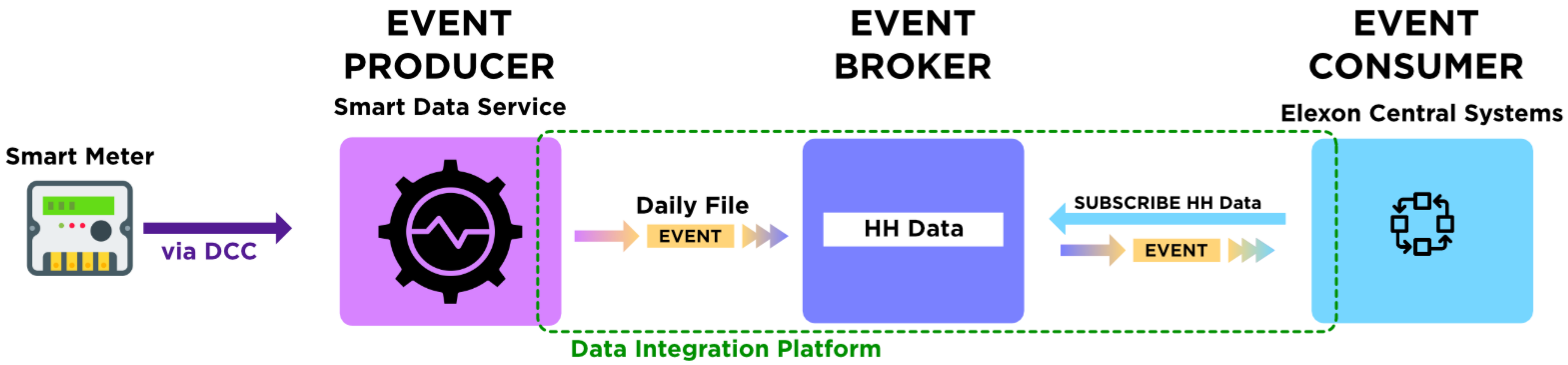
SUBSCRIBE TOPIC...

EVENT

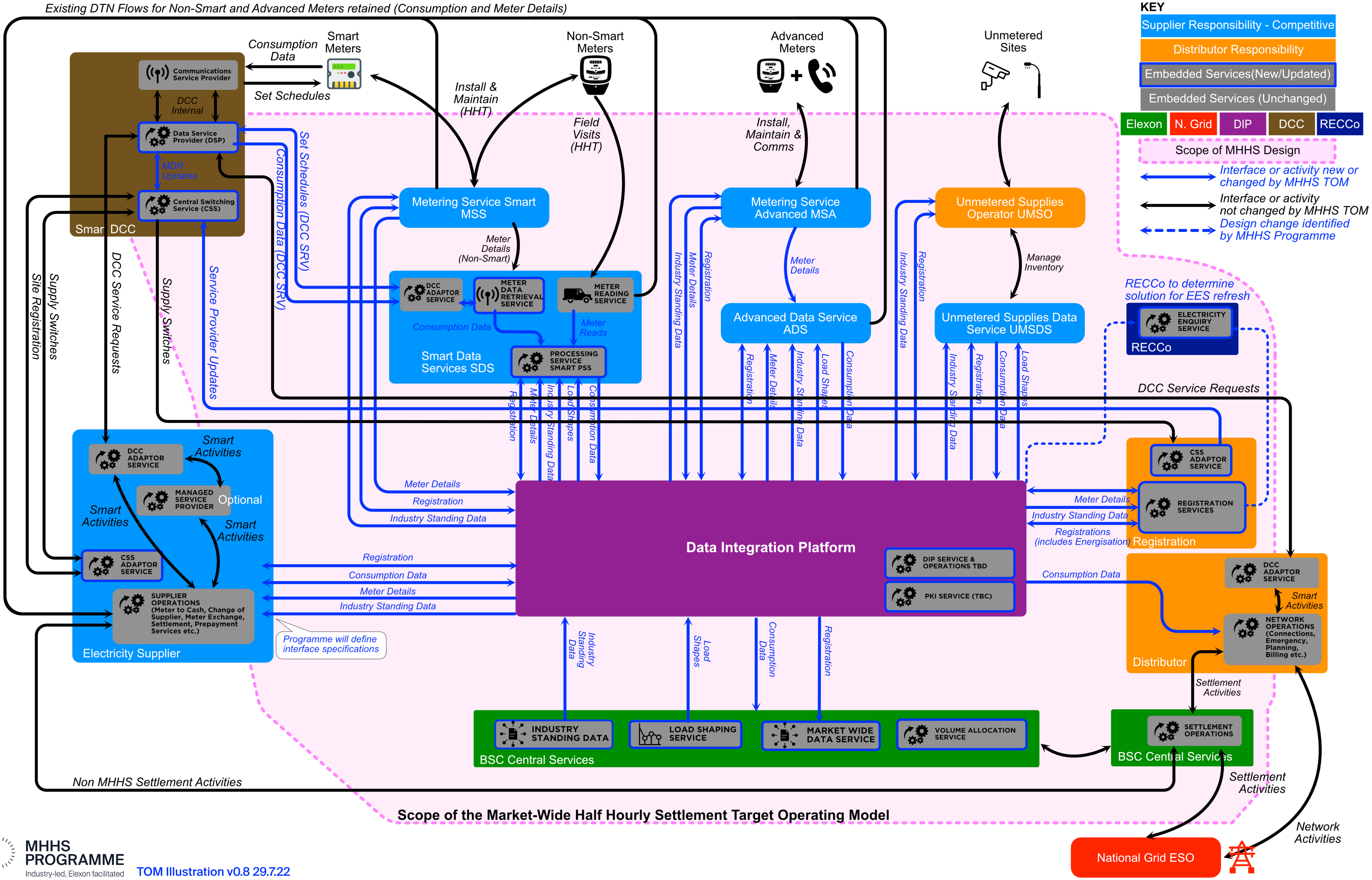
EVENT CONSUMER(S)

Questions - slido.com #MHHSTechnical

Deep Dive – Technical: Background #3



Questions - slido.com #MHHSTechnical



Existing DTN Flows for Non-Smart and Advanced Meters retained (Consumption and Meter Details)

KEY

Supplier Responsibility - Competitive

Distributor Responsibility

Embedded Services(New/Updated)

Embedded Services (Unchanged)

Elexon | N. Grid | DIP | DCC | RECCo

Scope of MHHS Design

Interface or activity new or changed by MHHS TOM

Interface or activity not changed by MHHS TOM

Design change identified by MHHS Programme

Smart DCC: Communications Service Provider; DCC Internal; Data Service Provider (DSP); MDR Updates; Central Switching Service (CSS)

Smart Meters; Consumption Data; Set Schedules

Non-Smart Meters; Install & Maintain (HHT); Field Visits (HHT)

Advanced Meters; Install, Maintain & Comms

Unmetered Sites

Metering Service Smart MSS

Meter Details (Non-Smart)

Smart Data Services SDS: DCC Adaptor Service; Meter Data Retrieval Service; Meter Reading Service; Meter Reads; Consumption Data; Processing Service Smart PSS

Set Schedules (DCC SRV)

Consumption Data (DCC SRV)

Metering Service Advanced MSA

Meter Details

Advanced Data Service ADS

Unmetered Supplies Operator UMSO

Manage Inventory

Unmetered Supplies Data Service UMSDS

RECCo to determine solution for EES refresh

RECCo: Electricity Enquiry Service

DCC Service Requests

Site Registration; Supply Switches; DCC Service Requests; Supply Switches; Service Provider Updates

Registration; Meter Details; Industry Standing Data; Load Shapes; Consumption Data

Electricity Supplier: DCC Adaptor Service; Smart Activities; Managed Service Provider; Optional; Smart Activities; Smart Activities; CSS Adaptor Service; Supplier Operations (Meter to Cash, Change of Supplier, Meter Exchange, Settlement, Prepayment Services etc.)

Meter Details; Registration; Industry Standing Data

Registration; Consumption Data; Meter Details; Industry Standing Data

Programme will define interface specifications

Data Integration Platform: DIP Service & Operations TBD; PKI Service (TBC)

Meter Details; Industry Standing Data; Registrations (includes Energisation)

Registration: CSS Adaptor Service; Registration Services

Consumption Data

Distributor: DCC Adaptor Service; Smart Activities; Network Operations (Connections, Emergency, Planning, Billing etc.)

Industry Standing Data; Load Shapes; Consumption Data; Registration

BSC Central Services: Industry Standing Data; Load Shaping Service; Market Wide Data Service; Volume Allocation Service

Settlement Activities

BSC Central Services: Settlement Operations

Settlement Activities

Network Activities

National Grid ESO

Non MHHS Settlement Activities

Scope of the Market-Wide Half Hourly Settlement Target Operating Model

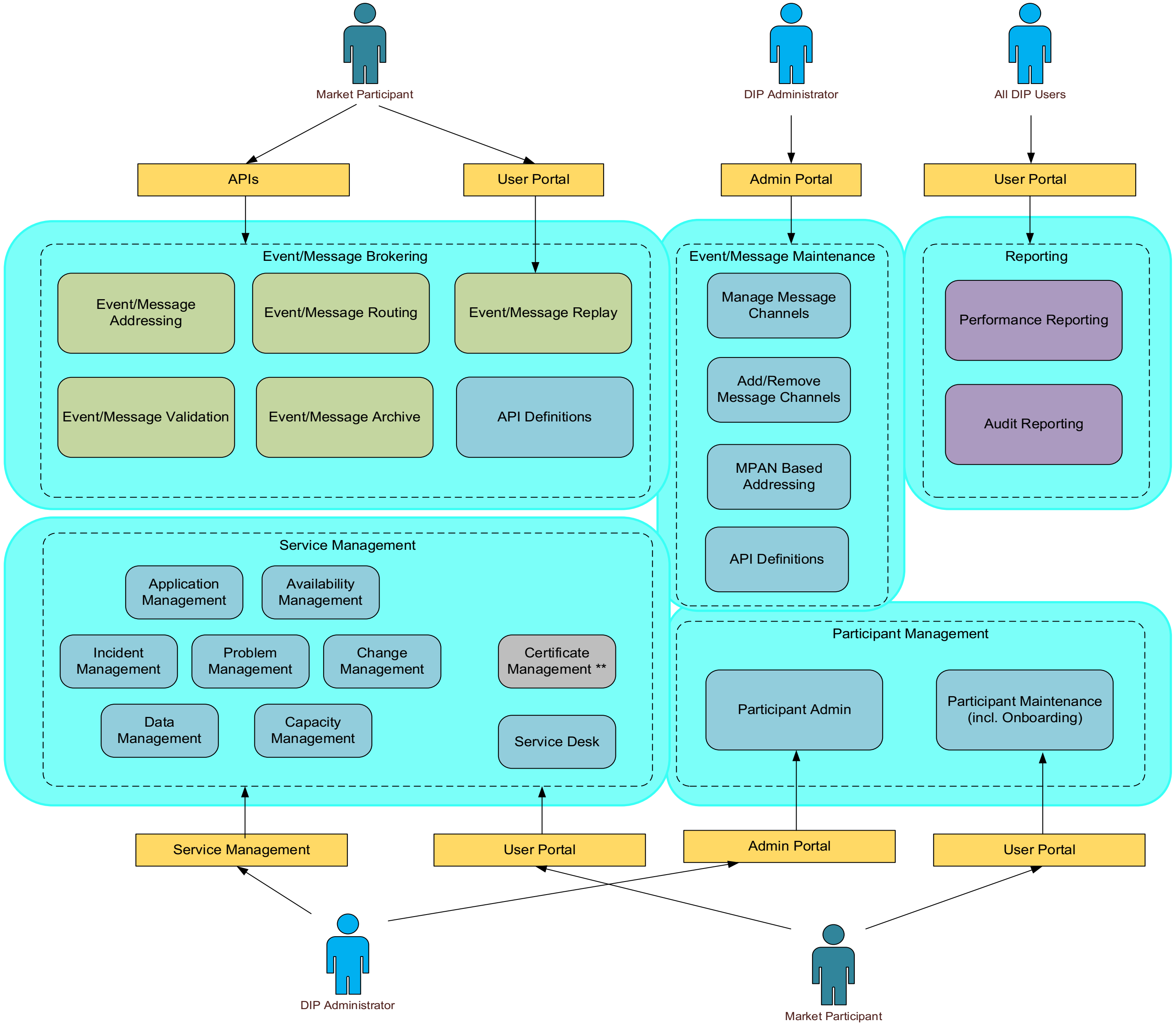
MHHS PROGRAMME

Industry-led, Elexon facilitated

TOM Illustration v0.8 29.7.22

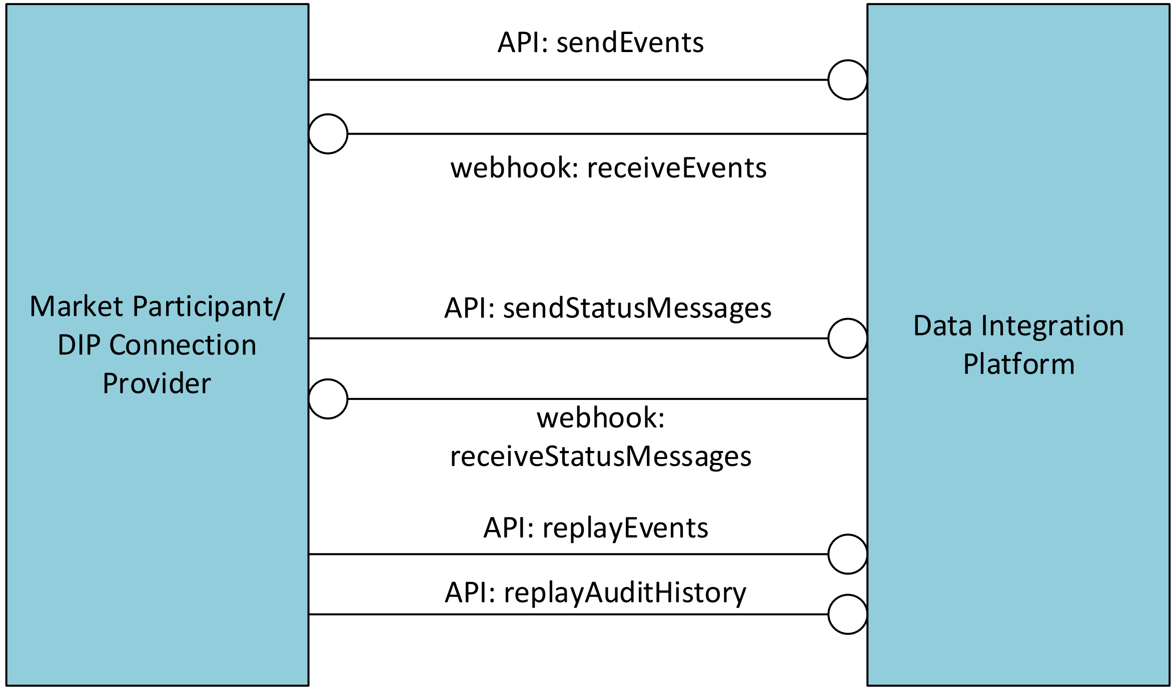
Deep Dive – Technical: DIP Overview

Questions - slido.com #MHHSTechnical



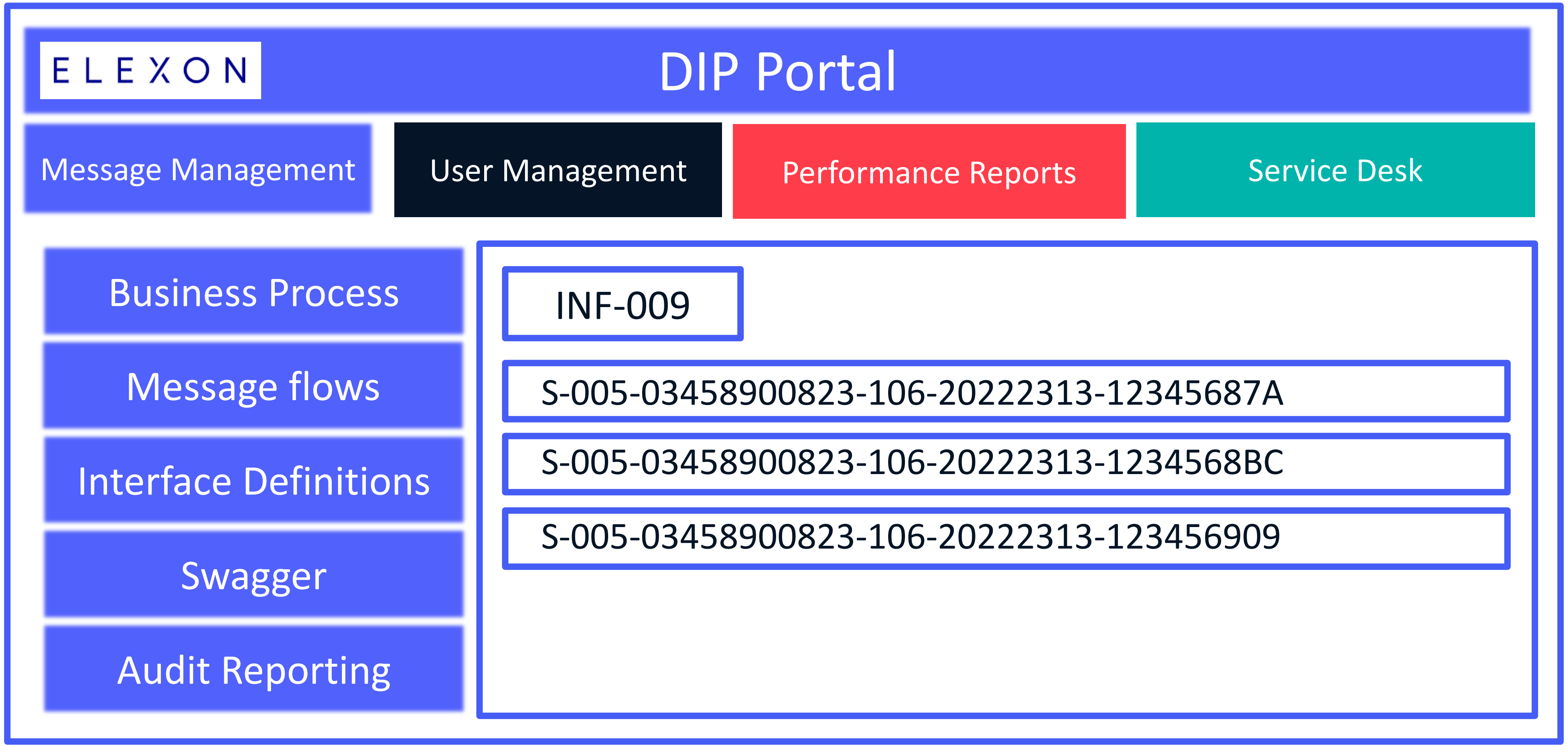
MHHS PROGRAMME
Industry-led, Elexon facilitated

Deep Dive – Technical: Market Participant to DIP Interfaces (automated)



1.	Send Events	API	Send messages/events to Market Participants via the DIP
2.	Receive Events	Webhook	Receive messages/events from the Market Participants via the DIP
3.	Send Status Messages	API	Send status (error) messages back to Market Participants via the DIP
4.	Receive Status Messages	Webhook	Receive status messages from Market Participants
5.	Replay Events	API	Request and receive replay of archived messages/events
6	Replay Audit History	API	Request Message audit history

Deep Dive – Technical: Market Participant User Interface



ELEXON

DIP Portal

Message Management

User Management

Performance Reports

Service Desk

Business Process

Message flows

Interface Definitions

Swagger

Audit Reporting

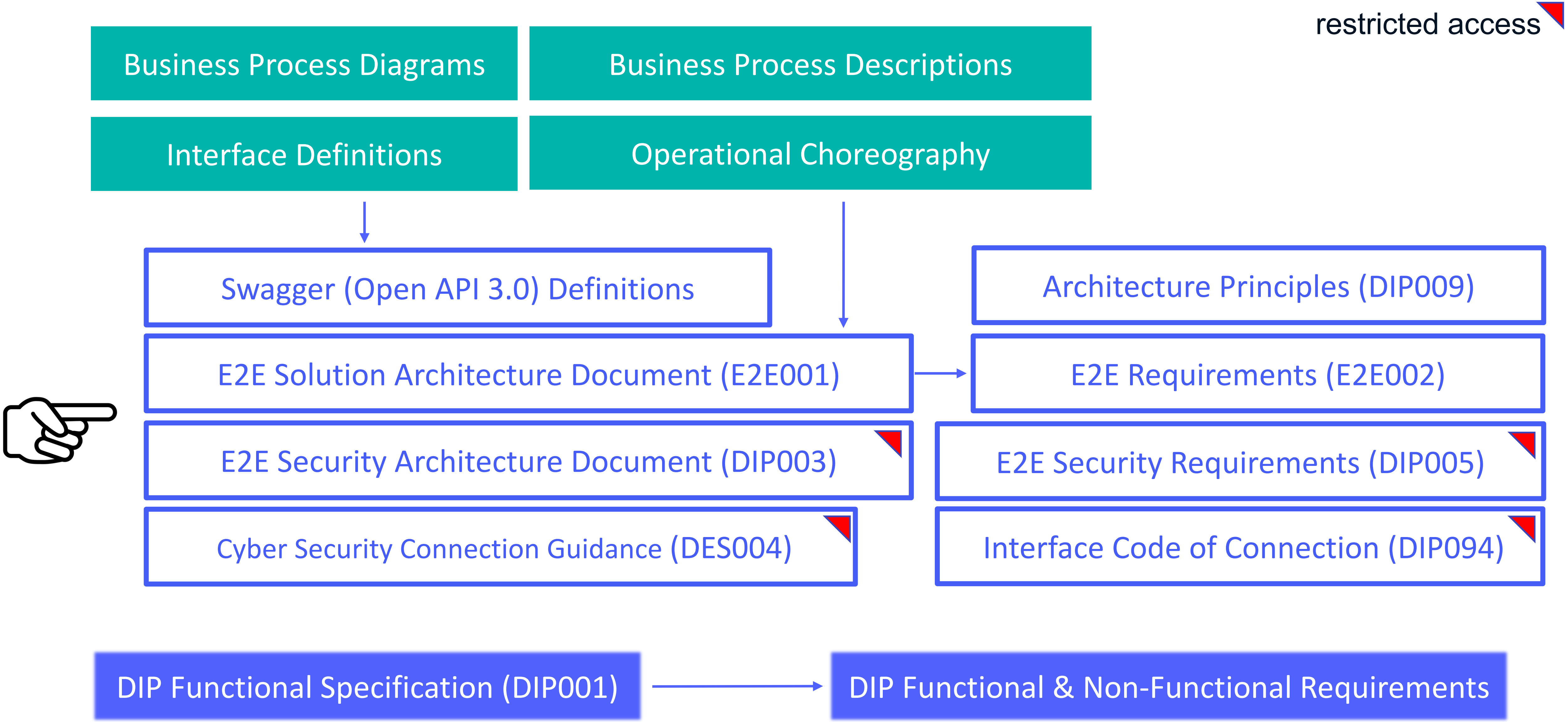
INF-009

S-005-03458900823-106-20222313-12345687A

S-005-03458900823-106-20222313-1234568BC

S-005-03458900823-106-20222313-123456909

Deep Dive – Technical: Documentation



restricted access

Business Process Diagrams

Business Process Descriptions

Interface Definitions

Operational Choreography

Swagger (Open API 3.0) Definitions

Architecture Principles (DIP009)

E2E Solution Architecture Document (E2E001)

E2E Requirements (E2E002)

E2E Security Architecture Document (DIP003)

E2E Security Requirements (DIP005)

Cyber Security Connection Guidance (DES004)

Interface Code of Connection (DIP094)

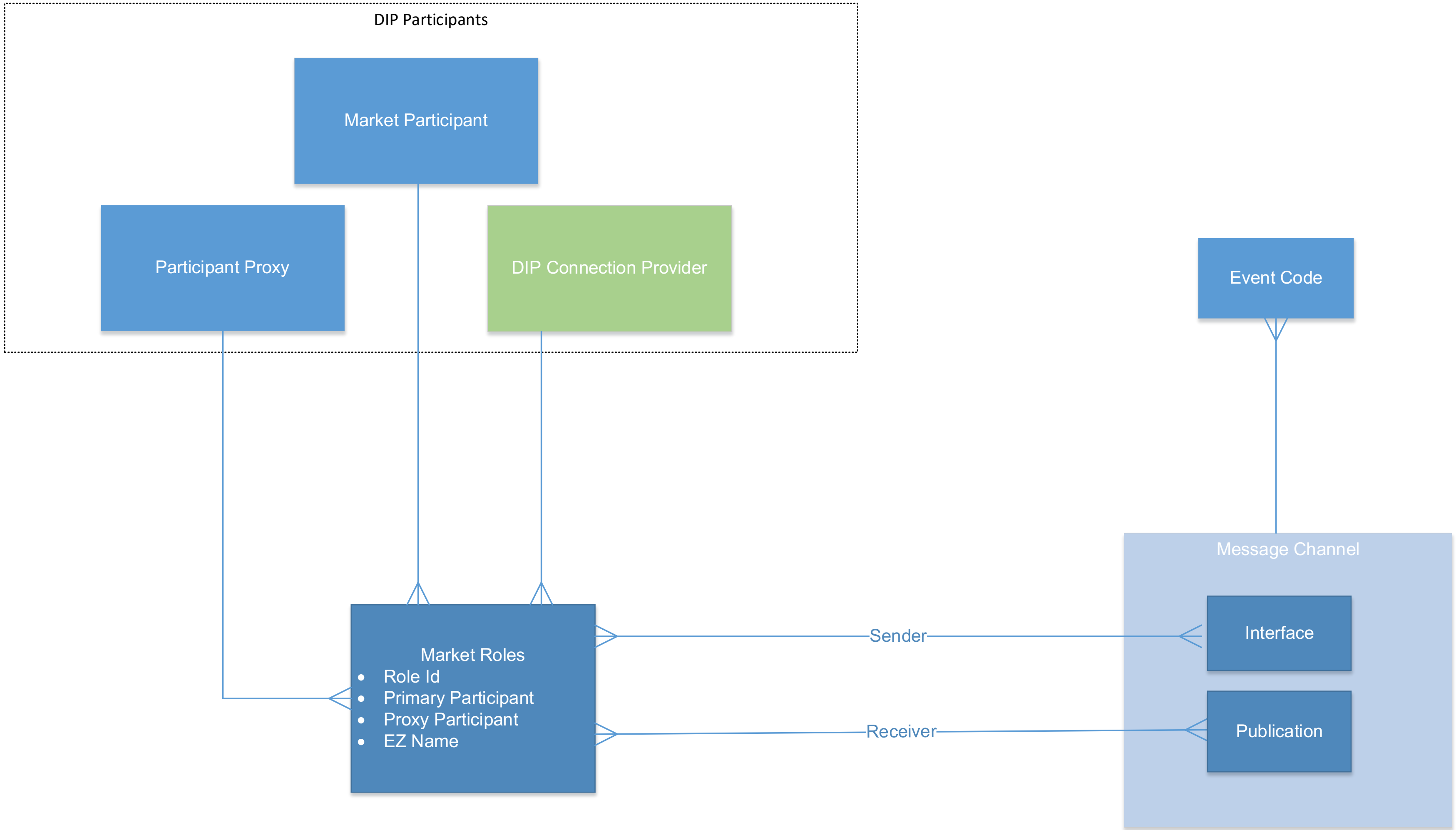
DIP Functional Specification (DIP001)

DIP Functional & Non-Functional Requirements

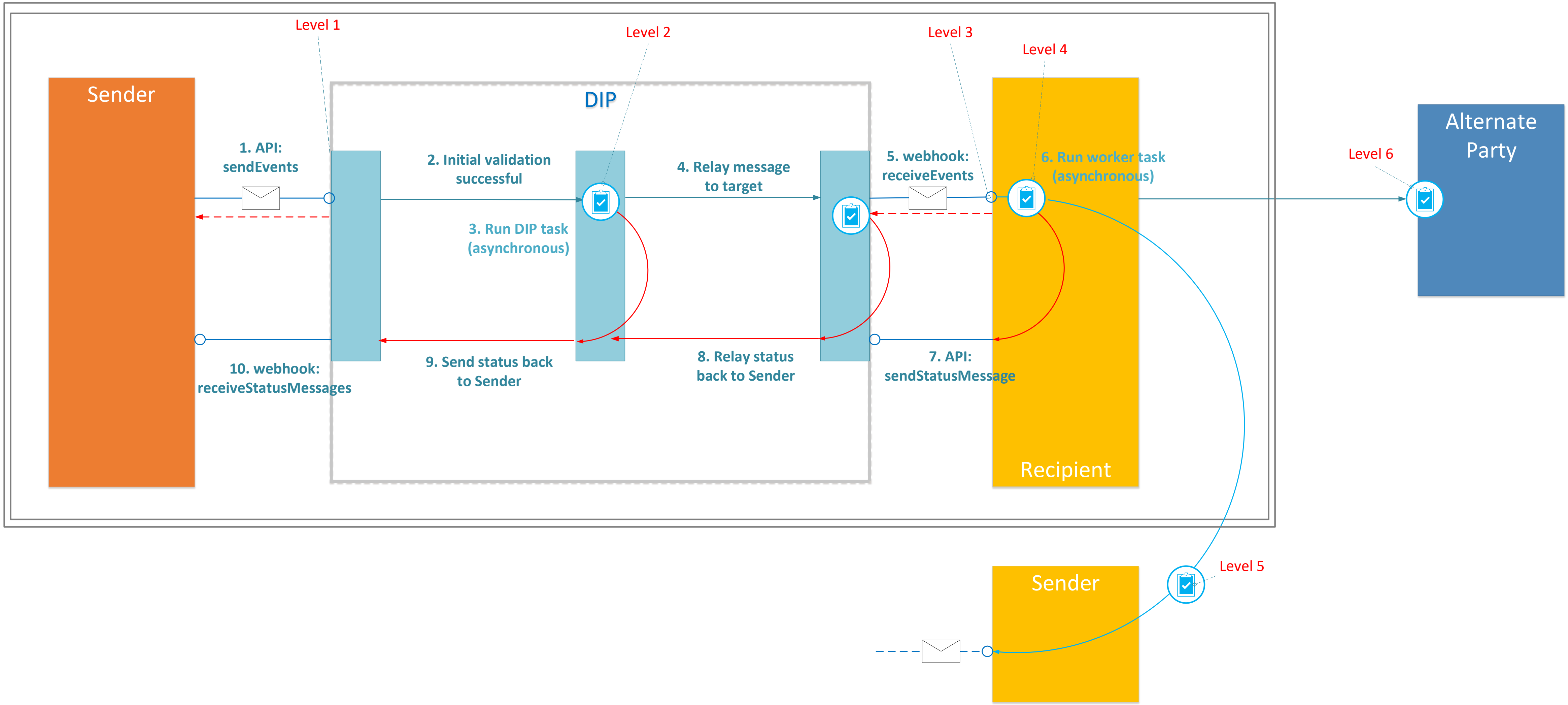
Questions - slido.com #MHHSTechnical

Deep Dive – Technical: DIP Participants On-boarding

Questions - slido.com #MHHSTechnical



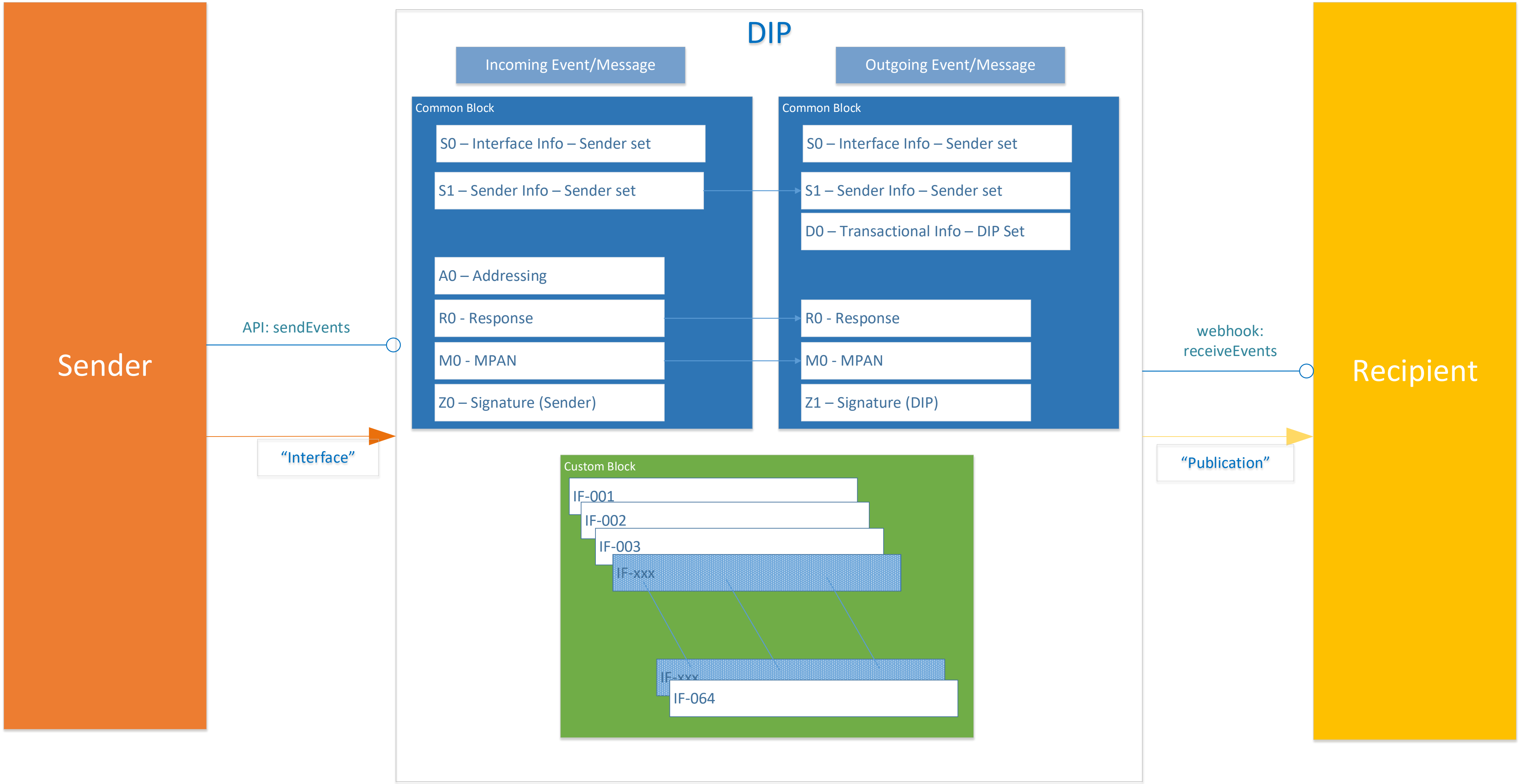
Deep Dive – Technical: Message Journey


Level 1
Level 2
Level 3
Level 4
Sender
DIP
1. API: sendEvents
2. Initial validation successful
3. Run DIP task (asynchronous)
4. Relay message to target
5. webhook: receiveEvents
6. Run worker task (asynchronous)
Level 6
Alternate Party
10. webhook: receiveStatusMessages
9. Send status back to Sender
8. Relay status back to Sender
7. API: sendStatusMessage
Recipient
Level 5
Sender

MHHS PROGRAMME
Industry-led, Elexon facilitated

Questions - slido.com #MHHSTechnical

Deep Dive – Technical: Message Formats



Sender

API: sendEvents

“Interface”

DIP

Incoming Event/Message

Common Block

S0 – Interface Info – Sender set

S1 – Sender Info – Sender set

A0 – Addressing

R0 - Response

M0 - MPAN

Z0 – Signature (Sender)

Outgoing Event/Message

Common Block

S0 – Interface Info – Sender set

S1 – Sender Info – Sender set

D0 – Transactional Info – DIP Set

R0 - Response

M0 - MPAN

Z1 – Signature (DIP)

Custom Block

IF-001

IF-002

IF-003

IF-xxx

IF-xxx

IF-064

webhook: receiveEvents

“Publication”

Recipient

Deep Dive – Technical: AWG Governance and Security

Events can be technically validated. They can be compared to allowed schema's and action can be taken in case of issues.

GDPR or sensitive data can be encrypted and access to topics storing sensitive data can be restricted and managed appropriately.

Data policies can be enforced by performing actions on events as they are published.

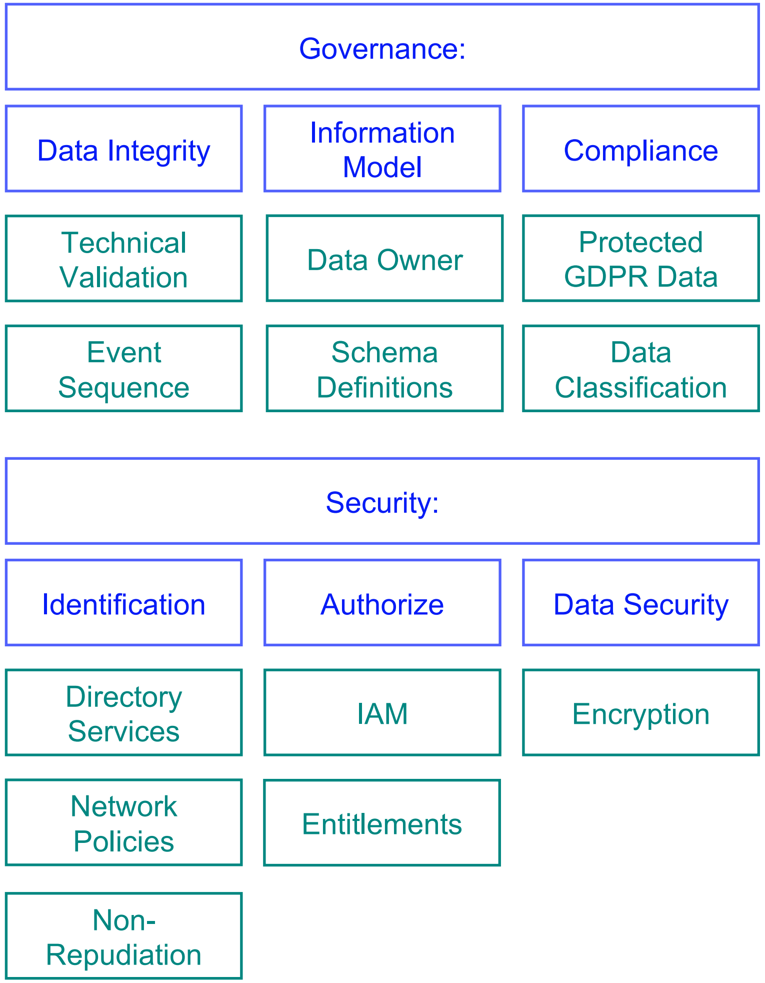
Data producers must be identified, authorized, and their data entitlements for publishing into topics should be validated.

Network security can be used to control inbound connections.

Data must be secure in transit (for example, using TLS) and at rest in the store.

Only valid data consumers may access events from restricted topics.

Entitlements to resources (such as the schema manager) can be managed, for example through ACLs.



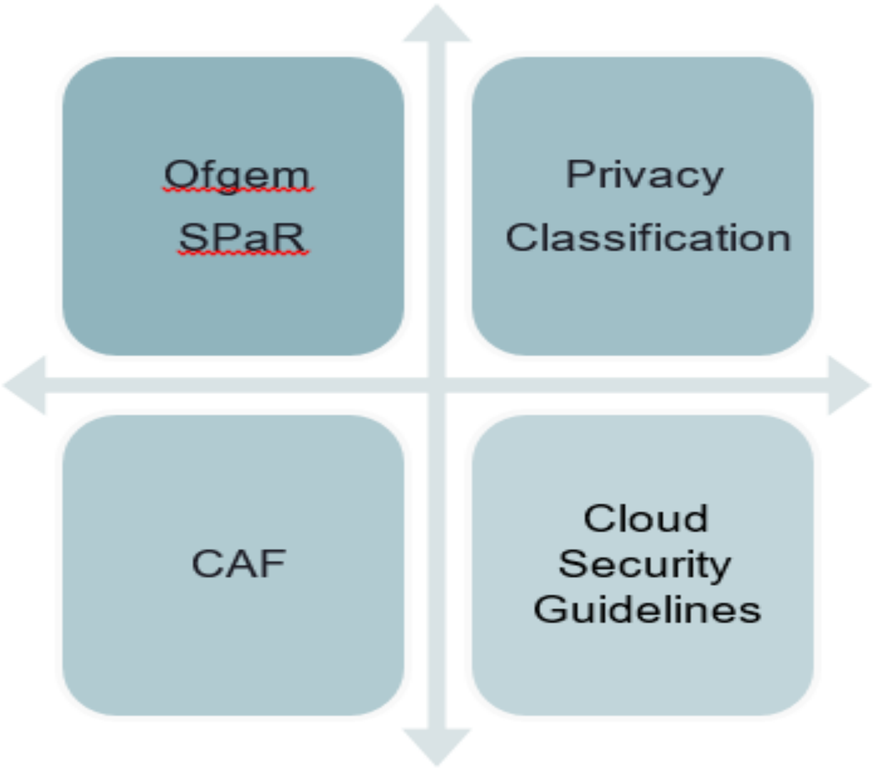
Governance:

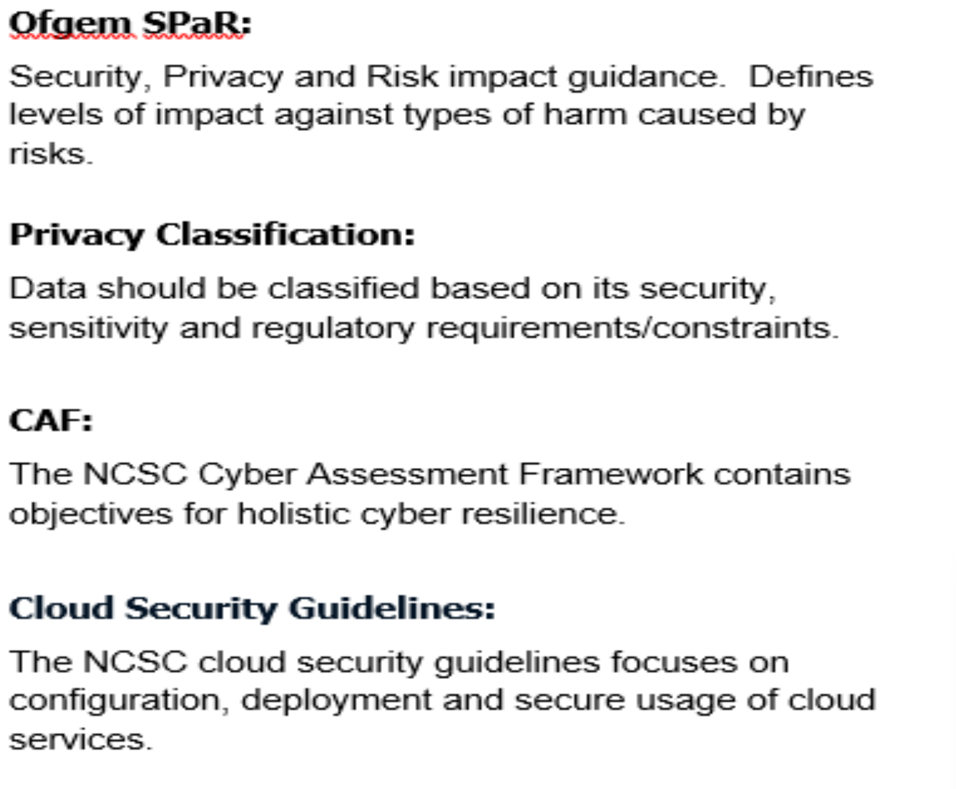
Data Integrity
Information Model
Compliance
Technical Validation
Data Owner
Protected GDPR Data
Event Sequence
Schema Definitions
Data Classification

Security:

Identification
Authorize
Data Security
Directory Services
IAM
Encryption
Network Policies
Entitlements
Non-Repudiation

Deep Dive – Technical: AWG Recommendations





Ofgem SPaR:

Security, Privacy and Risk impact guidance. Defines levels of impact against types of harm caused by risks.

Privacy Classification:

Data should be classified based on its security, sensitivity and regulatory requirements/constraints.

CAF:

The NCSC Cyber Assessment Framework contains objectives for holistic cyber resilience.

Cloud Security Guidelines:

The NCSC cloud security guidelines focuses on configuration, deployment and secure usage of cloud services.

Questions - slido.com #MHHSTechnical

Deep Dive – Technical: Secure connections

Messages

Detailed discussions were held with Ofgem regarding the levels of security that would need to be applied to messages being routed via the DIP.

The levels of security agreed upon by Ofgem, SDWG and the design team are:

- mTLS for Physical connectivity
- Digital signatures for integrity and non-repudiation

DPIA

Ofgem advised all parties sending and receiving messages via the DIP would require a valid and up to date DPIA that covers the data in scope.

- The ESO will verify the DPIA during the on-boarding process
- The ESO will ensure there is a DPIA for the DIP

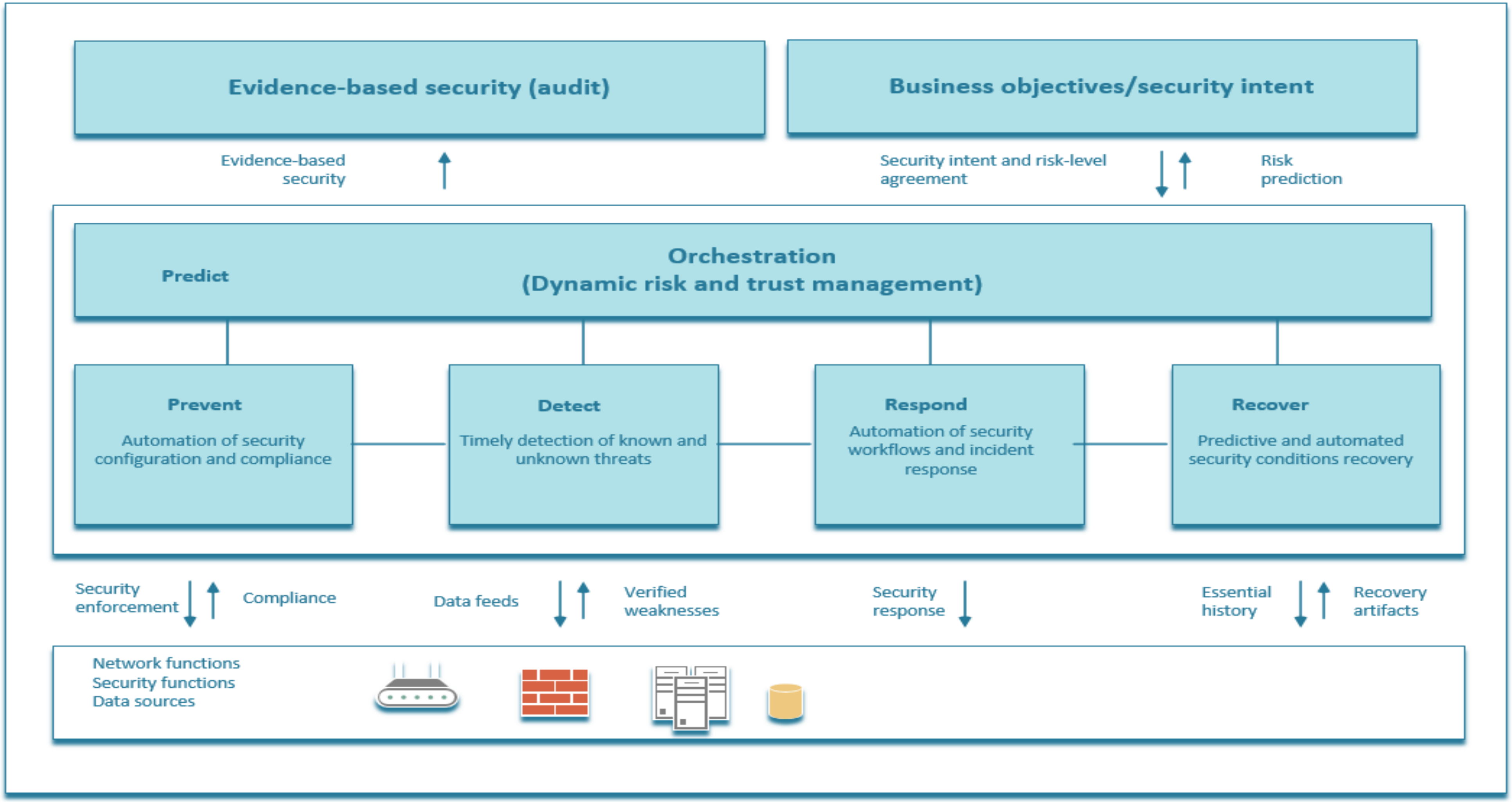
Risk Assessment

Where a Market Participant already has an up to date risk assessment such as those undertaken as part of the on-boarding process to RECAS, SECAS or the BSCCo no additional risk assessments or minimum security controls need to be applied providing the risk assessment includes the technology that the Market Participant will use for connectivity to the DIP.

- Where the risk assessment does not include the technology to be used for connectivity to the DIP a risk assessment and minimum security controls would be required as per the on-boarding process of the BSC Code.

Deep Dive – Technical: End to End Security Architecture

Adaptive Security



Evidence-based security (audit)
Business objectives/security intent
Evidence-based security
Security intent and risk-level agreement
Risk prediction
Predict
Orchestration
(Dynamic risk and trust management)
Prevent
Automation of security configuration and compliance
Detect
Timely detection of known and unknown threats
Respond
Automation of security workflows and incident response
Recover
Predictive and automated security conditions recovery
Security enforcement
Compliance
Data feeds
Verified weaknesses
Security response
Essential history
Recovery artifacts
Network functions
Security functions
Data sources

MHHS PROGRAMME
Industry-led, Elexon facilitated

Deep Dive – Technical: End to End Security Requirements

Background

- The NCSC CAF is normally associated with Operators of Essential Services (OES) which fall under the Network and Information Systems Regulations (NISR).
  - The DIP is not an Operator of essential services and as such has no reporting requirement under NISR.
  - The NCSC CAF is not a detailed security framework and does not lend itself well to defining detailed end to end security requirements.
- The NCSC Cloud Principles provide good guidance but again are not a detailed security framework.

Approach

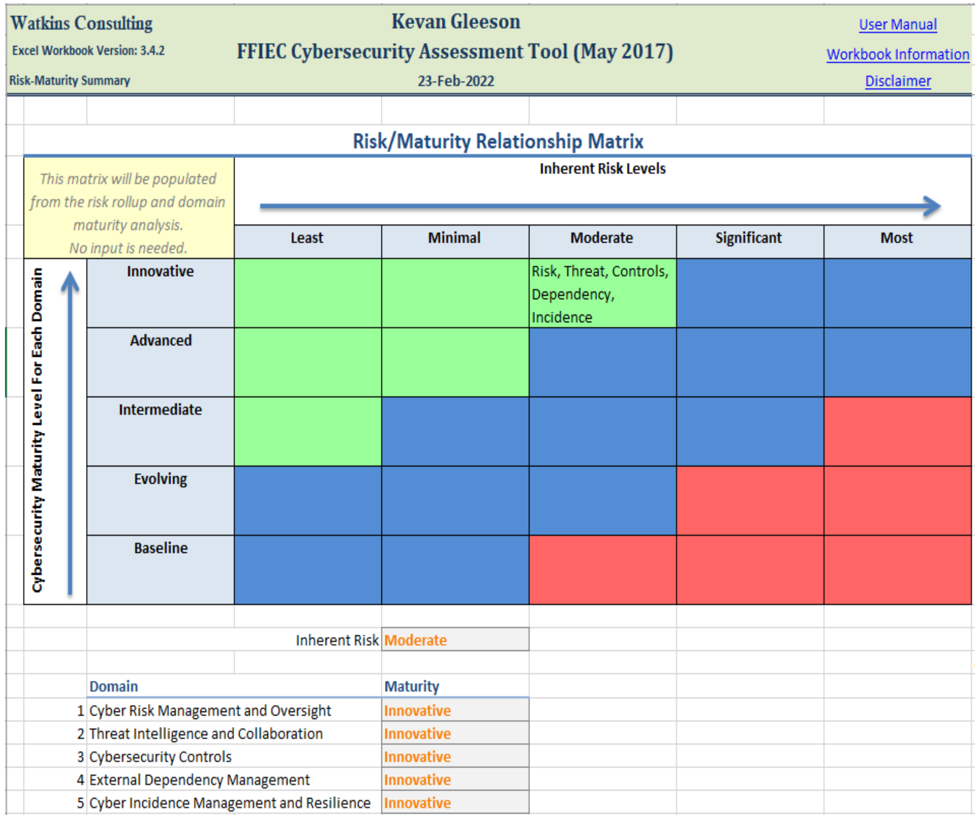
- Both the Center for Internet Security (CIS) Control Framework and the NIST Cyber Security Frameworks are recognized as industry standard frameworks when looking for detailed security controls.
- The DIP security requirements were produced and mapped against the following frameworks;
  - CIS v7.1 – Primary Control set due to CIS already being mapped against the MITRE Att&ck Framework
  - NIST v1.1 – Has already been mapped to NCSC CAF

Risk Assessments

- Threat use cases were developed based on the MITRE Att&ck Framework which was mapped back to the DIP Security requirements via the CIS Control Framework.
- The threat use cases were used to model risk to the DIP in a technical risk assessment tool based on IEC 62443-3-2.
- A more business focused risk assessment was undertaken using a freely available risk assessment tool from Watkins called the FFIEC-Cyber-Assessment-Tool-v3.4.2 tool.

Deep Dive – Technical: Risk Assessment

Watkins FFIEC Cyber Security Assessment tool.



Watkins Consulting

Excel Workbook Version: 3.4.2

Risk-Maturity Summary

Kevan Gleeson

FFIEC Cybersecurity Assessment Tool (May 2017)

23-Feb-2022

User Manual

Workbook Information

Disclaimer

Risk/Maturity Relationship Matrix

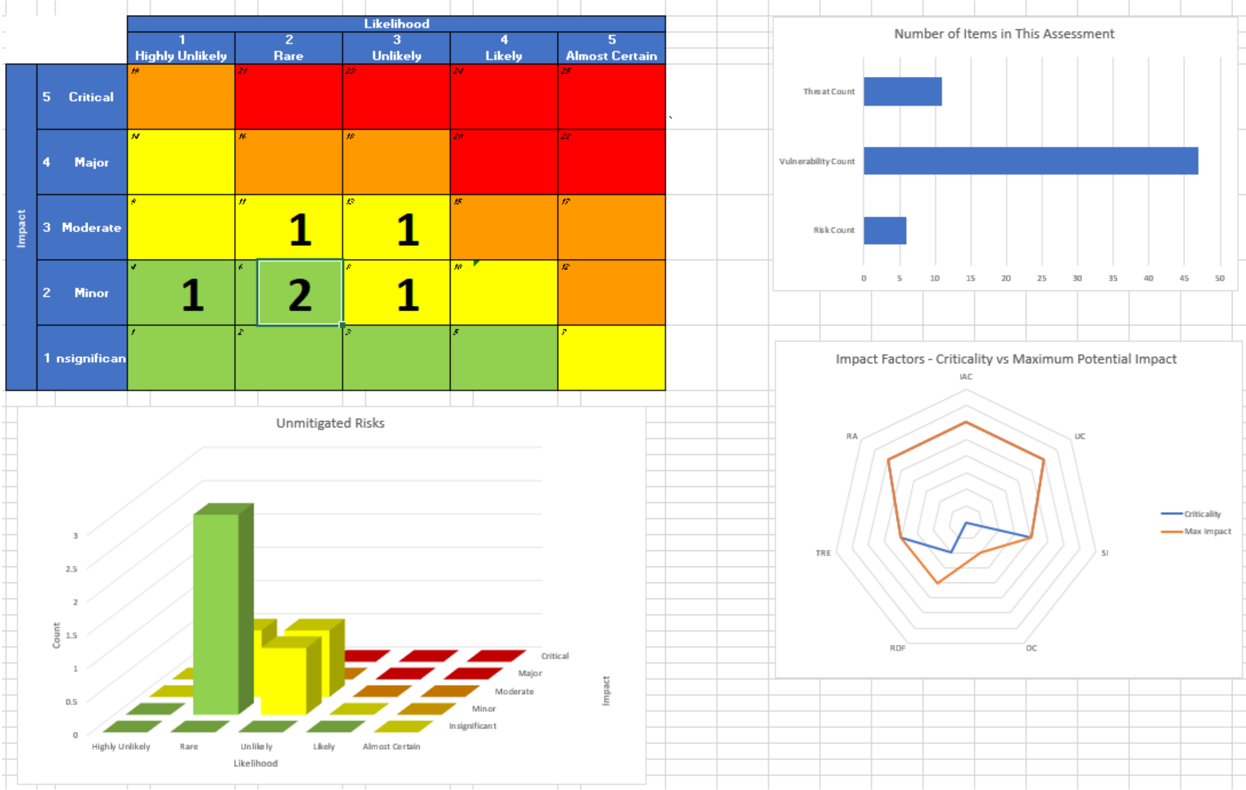
This matrix will be populated from the risk rollup and domain maturity analysis. No input is needed.

Cybersecurity Maturity Level For Each Domain	Inherent Risk Levels: Least	Minimal	Moderate	Significant	Most
Innovative	🟩	🟩	Risk, Threat, Controls, Dependency, Incidence	🟦	🟦
Advanced	🟩	🟩	🟦	🟦	🟦
Intermediate	🟩	🟦	🟦	🟦	🟥
Evolving	🟦	🟦	🟦	🟥	🟥
Baseline	🟦	🟦	🟥	🟥	🟥

Inherent Risk Moderate

	Domain	Maturity
1	Cyber Risk Management and Oversight	Innovative
2	Threat Intelligence and Collaboration	Innovative
3	Cybersecurity Controls	Innovative
4	External Dependency Management	Innovative
5	Cyber Incidence Management and Resilience	Innovative

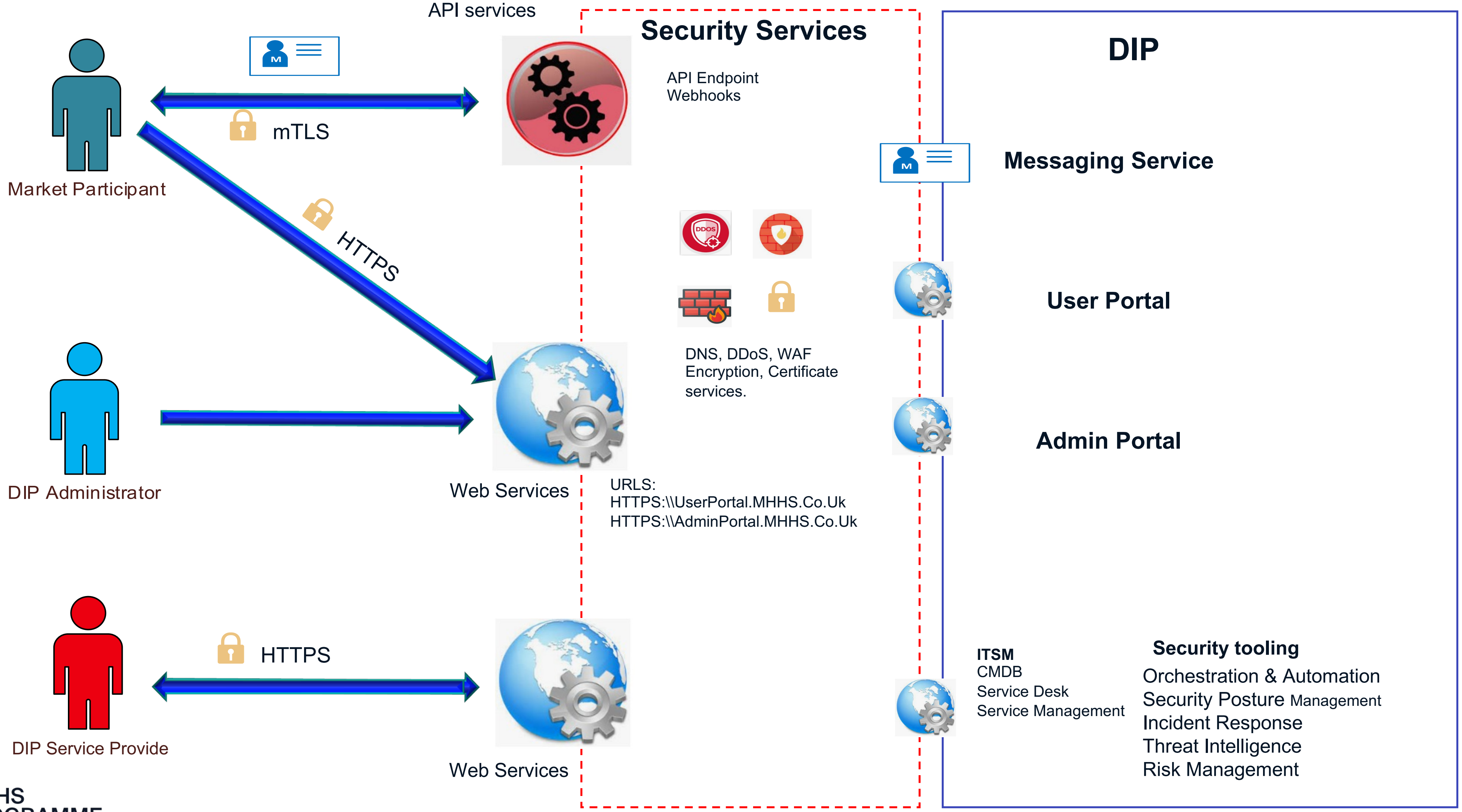
IEC 62443-3-2 Risk Assessment Tool



Impact		Likelihood: 1 Highly Unlikely	2 Rare	3 Unlikely	4 Likely	5 Almost Certain
	5 Critical	19	21	23	24	25
	4 Major	14	16	18	20	22
	3 Moderate	9	11 1	13 1	15	17
	2 Minor	4 1	6 2	8 1	10	12
	1 nsignifican	1	2	3	5	7

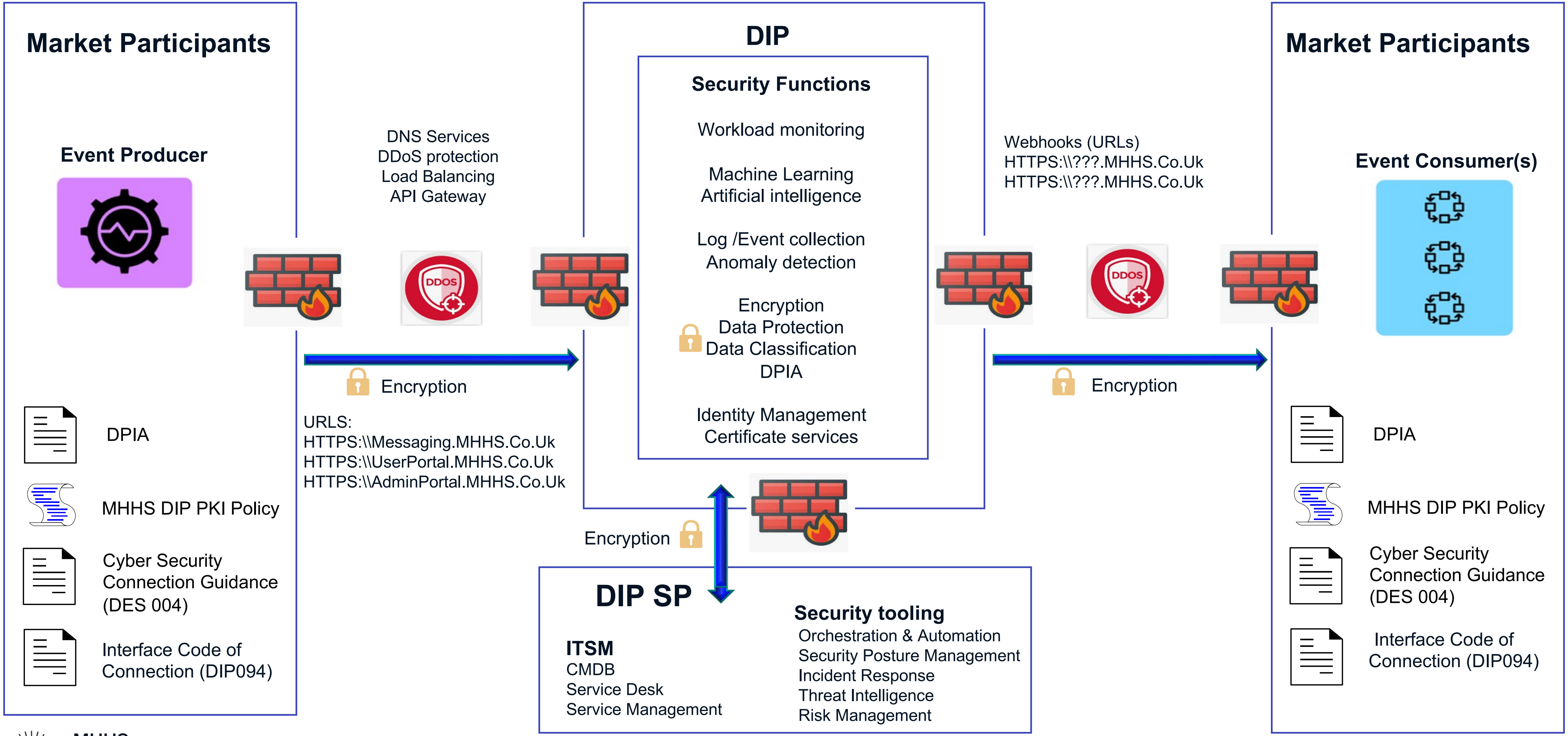
Deep Dive – Technical: DIP Interfaces

Questions - slido.com #MHHSTechnical



Deep Dive – Technical: Security Overview

Questions - slido.com #MHHSTechnical



Market Participants

Event Producer

DPIA

MHHS DIP PKI Policy

Cyber Security Connection Guidance (DES 004)

Interface Code of Connection (DIP094)

DNS Services
DDoS protection
Load Balancing
API Gateway

Encryption

URLS:
HTTPS:\\Messaging.MHHS.Co.Uk
HTTPS:\\UserPortal.MHHS.Co.Uk
HTTPS:\\AdminPortal.MHHS.Co.Uk

DIP

Security Functions

Workload monitoring

Machine Learning
Artificial intelligence

Log /Event collection
Anomaly detection

Encryption
Data Protection
Data Classification
DPIA

Identity Management
Certificate services

Encryption

DIP SP

ITSM
CMDB
Service Desk
Service Management

Security tooling
Orchestration & Automation
Security Posture Management
Incident Response
Threat Intelligence
Risk Management

Webhooks (URLs)
HTTPS:\\???.MHHS.Co.Uk
HTTPS:\\???.MHHS.Co.Uk

Encryption

Market Participants

Event Consumer(s)

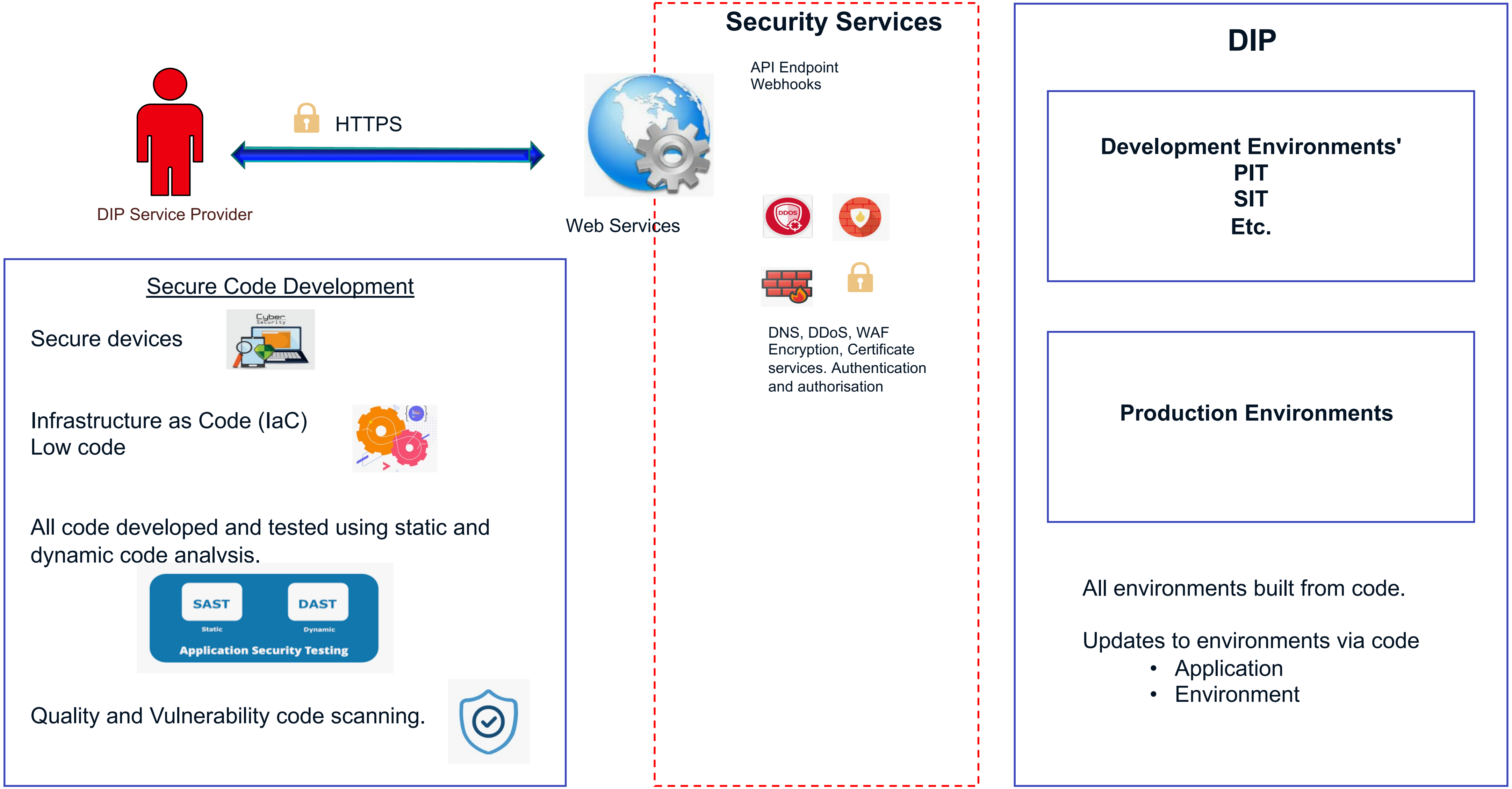
DPIA

MHHS DIP PKI Policy

Cyber Security Connection Guidance (DES 004)

Interface Code of Connection (DIP094)

Deep Dive – Secure application development



HTTPS

DIP Service Provider

Web Services

Security Services

API Endpoint
Webhooks

DNS, DDoS, WAF
Encryption, Certificate services. Authentication and authorisation

Secure Code Development

Secure devices

Infrastructure as Code (IaC)
Low code

All code developed and tested using static and dynamic code analysis.

SAST Static
DAST Dynamic
Application Security Testing

Quality and Vulnerability code scanning.

DIP

Development Environments'
PIT
SIT
Etc.

Production Environments

All environments built from code.

Updates to environments via code
- Application
- Environment

MHHS PROGRAMME
Industry-led, Elexon facilitated

Any questions?

Please join at Slido.com

#MHHSTechnical