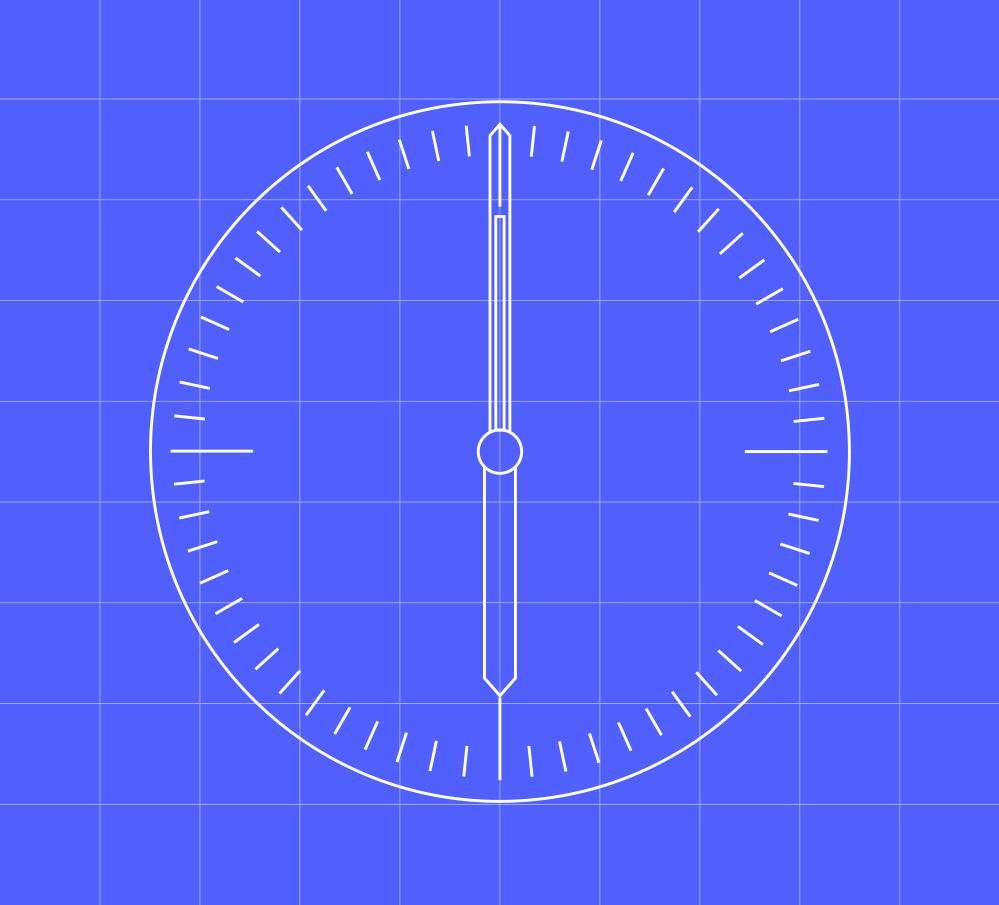
****MHHS Data Integration Platform –****

****End to End Security Architecture****



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document owner | Document number | Version | Status: | Date |
| **MHHS DAG** | **MHHS-DIP003** | **Version 1.2** | **Draft** | **03 Noember 2022** |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Document owner | Document number | Date |
|  |  |  |

# Table of Contents

[1 Table of Contents 2](#_Toc113958319)

[1.1 Change Record 3](#_Toc113958320)

[1.2 Reviewers 3](#_Toc113958321)

[1.3 References 3](#_Toc113958322)

[1.4 Terminology 4](#_Toc113958323)

[2 Background 4](#_Toc113958324)

[3 Introduction 5](#_Toc113958325)

[3.1 Data Integration Platform (DIP) 5](#_Toc113958326)

[4 Security Architecture Goals 7](#_Toc113958327)

[5 Software Development 8](#_Toc113958328)

[5.1 Define the key security policies 8](#_Toc113958329)

[5.2 Software development lifecycle 8](#_Toc113958330)

[5.2.1 SDLC phases: 9](#_Toc113958331)

[5.2.2 Advantages of a secure SDLC approach: 9](#_Toc113958332)

[6 End to End Security Architecture 9](#_Toc113958333)

[6.1 Adaptive security architecture 10](#_Toc113958334)

[6.2 Actors and trust 12](#_Toc113958335)

[6.2.1 Actors. 12](#_Toc113958336)

[6.2.2 Trust 13](#_Toc113958337)

[6.3 Domain security 14](#_Toc113958338)

[6.3.1 Navigating domain security 14](#_Toc113958339)

[6.3.2 Domain Communications (internal / external) 14](#_Toc113958340)

[6.3.3 Domain Security functions 14](#_Toc113958341)

[6.4 Asset management 15](#_Toc113958342)

[6.5 Vulnerability, threat and risk management 15](#_Toc113958343)

[6.6 Identity and access management 15](#_Toc113958344)

[6.6.1 Identity management 15](#_Toc113958345)

[6.6.2 Access control 16](#_Toc113958346)

[6.7 Security patterns (guardrails) 16](#_Toc113958347)

[6.8 Compliance monitoring 16](#_Toc113958348)

[6.9 GDPR compliance 17](#_Toc113958349)

[6.10 Data loss prevention 17](#_Toc113958350)

[6.11 Response / Incident management 17](#_Toc113958351)

[6.12 End to End Security management and automation solution 17](#_Toc113958352)

[7 Deployment and operation of the security management solution. 18](#_Toc113958353)

[7.1 Provide cyber security services 18](#_Toc113958354)

[7.2 Enable advanced cyber security capabilities 20](#_Toc113958355)

[7.3 Develop a cyber-security empowered workforce 20](#_Toc113958356)

[7.4 Improve cyber security situational awareness 20](#_Toc113958357)

[7.5 Performance measurement: 21](#_Toc113958358)

[Appendix A – Business Flows, Message Routing and Digital signing 22](#_Toc113958359)

[Appendix B – End to End Security Requirements 24](#_Toc113958360)

[Appendix C – MHHS AWG Security Principles and Data Architecture Standards 24](#_Toc113958361)

## Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Detail |
| 10 November 2021 | KG | 0.1 | Initial Draft. |
| 16 December 2021 | KG | 0.2 | Updated to incorporate encryption patterns. |
| 07 February 2022 | KG | 0.3 | Updated based on feedback from peer review. |
| 17 February 2022 | KG | 0.4 | Updated based on SDWG feedback. |
| 20 February 2022 | KG | 0.5 | Updated based on feedback from Procurement |
| 27th July 2022 | KG | 1.0 | Set to version 1.0 |
| 13th September 2022 | KG | 1.1 | Removed references to message encryption. |
| 03rd November 2022 | KG | 1.2 | Updated Post SDWG Assurance Forum Review |

## Reviewers

|  |  |
| --- | --- |
| Reviewer | Role |
| Robert Golding | Solution Architect |
| Ian Smith | Design Manager |
| Security Design Working Group |  |

## References

|  |  |  |  |
| --- | --- | --- | --- |
| Document/Link | Publisher | Published | Additional Information |
| Distributed energy resources(der) cyber security connection guidance | Energy and networks association | n/a | The document does not state published date as of 01/11/2021 |
| MHHS 003 - AWG Principles 03 Security Guidelines v03 | AWG | 28 January 2020 |  |
| E2E Security requirements | DCC | 04/06/2018 |  |
| DOE IT security architecture | US Department of Energy | February 2007 |  |
| NCSC Cloud Principles | NCSC | The current version as of December 2021 | [Implementing the Cloud Security Principles - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles) |
| Cyber Assessment Framework | NCSC | CAF v3.0 | [Cyber Assessment Framework - NCSC.GOV.UK](https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework) |
| Data Best Practice  Supporting Information v0.3 | Proposed Version May 2021 |  | <https://www.ofgem.gov.uk/sites/default/files/docs/2021/05/data_best_practice_supporting_information_v0.3_0.pdf> |
| Oracle security in-depth - Whitepaper | Oracle | March 2013 | [Security In-Depth Reference Architecture (oracle.com)](https://www.oracle.com/technetwork/oracle-wp-security-ref-arch-1918345.pdf#page=7&zoom=100,125,723) |
| Ericsson - 5g core guide –network security | Ericsson | October 2020 | [Mastering complete 5G network security (ericsson.com)](https://www.ericsson.com/assets/local/digital-services/offerings/core-network/5g-core-guide-network-security.pdf?_ga=2.143320752.460970403.1643810635-337582871.1643810635) |
| ETSI GS NFV-SEC 013 | ETSI | V3.1.1 (2017-02) |  |

## Terminology

|  |  |
| --- | --- |
| Term | Description |
| AWG | Architecture Working Group |
| CAF | Cyber Assessment Framework (currently v3.0) |
| CSP | Cyber Security Programme |
| DAG | Design Advisory Group |
| DIP | Data Integration Platform |
| DIPSP | Data Integration Platform Service Provider |
| DPIA | Data Protection Impact Assessment |
| EDA | Event-Driven Architecture |
| FIM | File Integrity Monitoring |
| FIPS | Federal Information Processing Standards |
| HIDS | Host-Based Intrusion Detection |
| IGP | Indicators of Good Practice |
| ISO | Information Security Officer |
| ISP | Internet Service Provider |
| IT | Information Technology |
| MHHS | Market-wide Half Hourly Settlement |
| NCSC | National Cyber Security Centre |
| NIS | Network and Information Systems |
| NIST | National Institute of Standards and Technology |
| NIST SP | NIST Special Publication |
| SOAR | Security Orchestration Automation and Response |
| SSP | System Security Plan |
| TOM | Target Operating Model |
| UEBA | User and Entity Behaviour Analytics |
| XDR | Extended Threat Detection and Response |

# Background

Since 2018 Ofgem has hoped that Half-Hourly Settlement (HHS) on a market-wide basis would be introduced into the UK electricity market. A cross-industry Design Working Group (DWG) was established to understand the feasibility of HHS and how it could be delivered. The DWG produced a Target Operating Model (TOM) that outlines the new ways of working to deliver HHS into the market (Reference Target Operating Model for Market-wide Half Hourly Settlement).

In conjunction with the DWG, and Architectural Working Group (AWG) was established to propose an IT architecture that could support the business process outlined in the TOM. The AWG recommendation was that an Event-Driven Architecture (EDA) be implemented (*Reference MHHS AWG Recommendation*). Hence, a new message orientated/event-driven middleware component is required – the Data Integration Platform (DIP) - to support the flow of events/messages between industry participants proposed by the EDA.

* See Appendix C - MHHS AWG Principles for Security and Data Architecture for further information.

The MHHS Programme was set up to continue the preparatory work undertaken by the DWG & AWG, refine the TOM further, and then oversee its delivery into the industry.

Consequently, the information relied upon in this document was necessarily conceptual and focused on alignment with Good Industry Practice. Therefore, this document needs to be read in conjunction with the End to End security requirements which provides a detailed listing of all security requirements.

# Introduction

The End to End Security Architecture document is one of the security artefacts developed to address the security strategies, constraints and risk management activities faced by the Market-wide Half-Hourly Programme (MHHS). Drawing on Good Industry Practice, the document was developed to identify the security architecture of the new Data Integration Platform (referred to as the DIP). The security architecture document will build upon the conclusions of:

1. AWG recommendations (Architecture, Alignment to SPaR and NSCC CAF & Cloud Principles)
2. End to End security requirements document.

The security requirements are fully defined in the MHHS DES004 – End to End Security Requirements document, an embedded word document.

The End to End Security Architecture has been described in a way that could:

* Inform the creation of procurement documentation; and
* Enable the development of the security services required to secure connectivity from the Market Participants, the DIP itself and the service provider of security services.

## Data Integration Platform (DIP)

Market-wide Half Hourly Settlement (MHHS) is a new market model that delivers both settlement period (SP) meter readings from smart meters and derives SP level data from meters where register readings (RR) can be accessed.

The MMHS DIP covers the “Meter to Bank” process for all Supplier Volume Allocation (SVA) Settlement Meters – i.e. all Settlement Meters connected to distribution networks. This includes:

* Meter Registration - the recording of information pertinent to Settlement Metering Systems;
* Meter Operations - fitting and maintaining Settlement Meters;
* Data Retrieval - getting information from Settlement Meters;
* Data Processing – validating and estimating Settlement Meter data;
* Data Aggregation - summing Settlement Meter data to required granularity; and
* Volume Allocation – allocating Meter volumes to Trading Parties that are signatories to the BSC.

Figure 1represents alogical overview of how the DIP will look; a full description of the DIP is found in the MHHS DES001 – Functional Specification.



Figure 1 – Logical overview of the DIP

A service orientated view of the DIP is presented below in figure 2:



Figure 2 - Service Orientated View of the DIP

Figure 3 (below)represents alogical overview of how connectivity to the DIP could look, with MHHS PKI Certificate services provided by the DIP service provider.

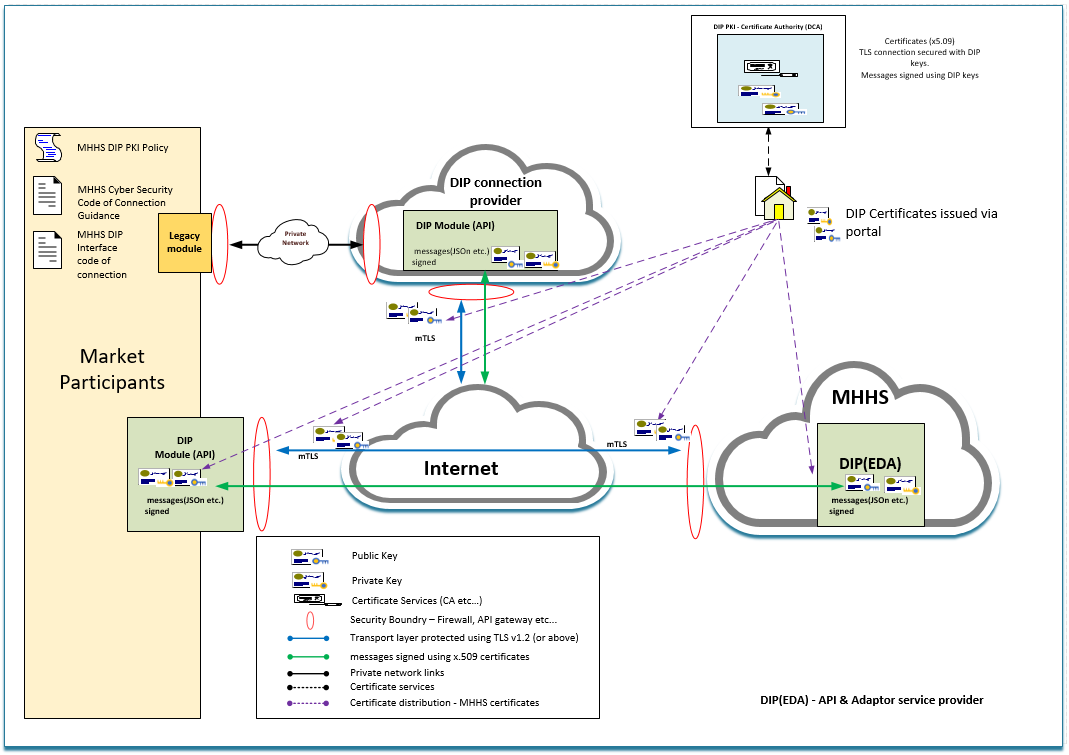


Figure 3 - Logical overview of the DIP connectivity.

# Security Architecture Goals

The end to end security architecture aims to protect the DIP and Market participants ensuring confidentiality, integrity, and availability of the DIP is protected commensurate with the needs, information value, and associated threats.

Data protection must begin with the creation of information, with a particular focus on defining and documenting protection levels and access control decisions. Protection must be assured throughout the life cycle of the data: creation, modification, storage, transport, and destruction. We can no longer rely simply on transport mechanisms/link encryption to provide our end-to-end protection. Information (e.g., data, metadata) will routinely flow in and out of the DIP through numerous access points (See figure 1 – Logical overview of the DIP and Appendix A Business flows). This separation of information from systems requires that the information must receive adequate protection, regardless of location. A critical factor in ensuring adequate protection for all data is the responsive updating and application of policy and guidance to address the latest changes in technologies while defending against the latest new and developing threats.

Equally important is the necessity to ensure that the policies and guidance provide sufficient flexibility to allow their adaptation across the DIP. In addition, achieving the goal of trusted data everywhere within the DIP requires partnerships and combined efforts with other components of the security community (i.e., Market Participant, service providers and third parties) to provide an integrated adaptive systems security posture. Cyber security policies define the requirements and procedures required to achieve the DIP's Cyber Security goals effectively.

# Software Development

Establish responsibility for security activities and expectations for behaviour, and set mandatory expectations related to software security.

## Define the key security policies

1. Software security. Build security into product requirements, implementation, procurement, deployment, and operations:

* Secure SDLC. Use is not optional.
* Application risk ranking. Identify where the most significant technical risk lies.
* Application design. Define security controls to be built into the DIP based on this document and the detailed security requirements.
* Application development. Require specific technology stacks and mandatory coding standards. Adhere to software secure-by-design principles such as OWASP / Microsoft SDL.
  + Application testing. defined schedules and testing intervals for:
    - Static and dynamic code evaluation.
    - White box / black box testing
* Defect severity and remediation. Establish rules for setting bug and flaw severities and timelines for fixing coding bugs and design flaws.

1. Network security. Determine protocols and authorisation levels to help define the DIP security.
2. Data security. Identify and classify sensitive data (MPaN, PII, Consumption data) apply the correct security features based on the data privacy classifications aligned to SPaR.
3. Virtual infrastructure security. Govern access control to secure the virtual infrastructure of the DIP.
4. Disaster recovery. Determine steps to take in the event of an attack, including reporting, recording, and resolution for attacks against applications.

## Software development lifecycle

Establish responsibility for security activities and expectations for behaviour, and set mandatory expectations related to software security.

The code developed for the DIP will be developed using secure coding standards (OWASP, CREST) and static code scanning tools (SAST) and software composition analysis (SCA) to understand better the impact of code on risks related to security.

All software development (application and cloud infrastructure) should follow a recognised software development lifecycle such as OWASP / Microsoft SDL.



Figure 4 – SDLC

### SDLC phases:

* Planning and requirements
* Architecture and design
* Test planning
* Coding
* Testing and results
* Release and maintenance.

### Advantages of a secure SDLC approach:

* Software is more secure, as security is a constant and ongoing concern.
* All stakeholders are aware of security considerations.
* Early detection of design flaws before they are coded into existence.
* Cost reduction, thanks to early detection and resolution of defects.
* Risk reduction of business risks.

# End to End Security Architecture

Security is never static; it is ever-changing.

Needs and requirements change, the threat landscape develops, and the risk appetite evolves, all of which can affect the security and privacy of the DIP. Building a secure and trustworthy service for the Market Participants has dependencies on all layers:

* secure application development (Section 5)
* secure device standards (Section 6)
* secure deployment and operation. (Section 7)

Relying only on traditional prevent-and-detect perimeter defences and rule-based security, such as antivirus and firewalls, becomes less effective when the DIP’s primary communications with Market participants is via APIs.

Continuous monitoring of the DIP and its behaviour is the only way to detect threats before it is too late reliably.

The DIP system spans from the Market Participants via different network interfaces (APIs, Webhooks) to the cloud that hosts the platform and the service consumed by Market Participants. Each element of the chain must be considered when defining the E2E security architecture.

Security is driven by risk and continuous risk management. For the DIP it also has to do with building trust in the cloud infrastructure platform (anchors of trust) and deployment and operations. A risk-driven, adaptive security management approach with automation that can enhance security visibility into the DIP will be increasingly needed.

Security automation will play a critical role in ensuring continuous security compliance, threat detection and response. Security automation offers the capability to scale security functions easily and swiftly react to new risks. It will enable the DIP to be constantly protected by adapting the security posture to the evolving risk landscape (Hacktivists, insider threats, nation-state attacks, DDoS, Ransomware etc.)

All security services and tools used to secure the DIP must be standalone and transferrable along with the supporting artefacts, documentation, policies, standards and intelligence built into the solution.

Traditional security architecture, adaptive security architecture and cyber mesh architectures are all candidates for the DIP.

Table 1 below provides an overview of the applicability of the differing options.

|  |  |  |  |
| --- | --- | --- | --- |
| Security Architecture | Pros | Cons | Outcome |
| Traditional | Well established toolsets. | Cannot meet the changing needs of the DIP, Point solutions are resource-intensive to manage. | Least favourable option |
| Adaptive | Meets the changing needs of today’s cyber threats. Provides for greater automation, less dependent on human resources and expertise. | More costly than traditional security architectures to set up. | Preferred option |
| Mesh | A modern approach to a security architecture that caters for distributed enterprises. | Leading-edge, Cost, designed for more complex environments. | Gold plated solution. |

Table 1 – Security architecture

## Adaptive security architecture

An “Adaptive security architecture” is the preferred approach for the DIP.

The adaptive security architecture must leverage advanced security analytics and machine learning to provide a threat, risk and data security management. Therefore, the security solution chosen must take charge of the overall security, privacy policies, and compliance of the DIP by establishing managed identities and enforcing policies and security patterns (guardrails). Gartner’s 'four stages of adaptive security architecture is illustrated in Figure 4 below.



Figure 5 - ‘four stages of an adaptive security architecture’

The adaptive security architecture requires a comprehensive security and identity management solution that is able to manage and orchestrate the DIP components both ***horizontally*** (from device to service and service to user) and ***vertically*** (from cloud resources to application). In addition to this, the ability to address both security and identity from the Market participants to the DIP and all the way across the complete service life cycle will also be essential.

Figure 2 illustrates an adaptive approach to ‘security and identity management and highlights three key aspects:

1. security and identity management
2. security and identity functions
3. trust anchoring.

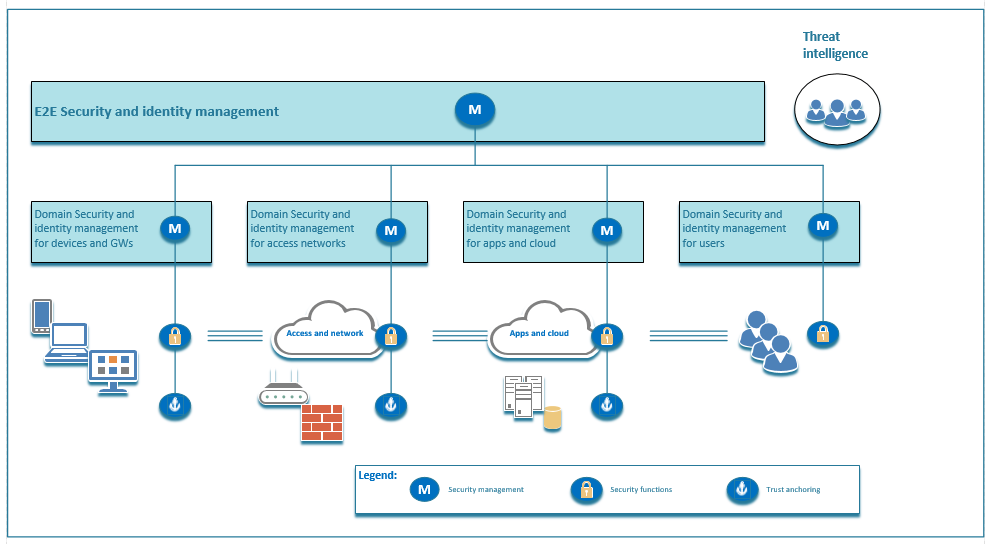


Figure 6 - E2E adaptive approach to security and identity management

## Actors and trust

### Actors.

In order to service the industry business flows (messaging services), the Market Participants, the DIP Service Provider and the devices used to deliver those services are all required to work collectively and securely.

In the adaptive security architecture, the Market Participants, the DIP Service Provider and the devices used to deliver the services are defined as ‘actors’ in this document; these actors all affect trust. Figure 3 (Below) illustrates the main and supporting actors and their trust relationships within the DIP.



Figure 7 - Actors and Trust relationship

The three main actors in the DIP solution are;

1. Market participants (Publisher Subscriber)
2. DIP Service Provider
3. Devices that enable the provision of the DIP service.

The supporting actors are;

1. The DIP Service Provider, whose role it is to provide the DIP application and cloud infrastructure (Azure, AWS, GCP etc.)
2. Connectivity to and from the Market participants and any DIP connection providers (third parties).

### Trust

The trustworthiness of services and ‘service users’ depends on how the actors (main and supporting) govern identities and data, security and privacy, and the degree to which they comply with the DIP’s policies and any regulatory requirements. Combining the security and identity functions is essential for defining the trust level.

An E2E approach is therefore essential to ensure trust among all actors in the DIP. Figure 4 illustrates a view of how security can be managed and deployed in an E2E manner throughout the DIP to monitor and protect system resources and assets. The architecture consists of an E2E security and identity management layer, security domains (device and gateway, access and networks, application and cloud infrastructure), specific management layers, and security and identity functions in each security domain component***.*** Figure 8 below illustrates an E2E approach to security and identity management for the DIP.

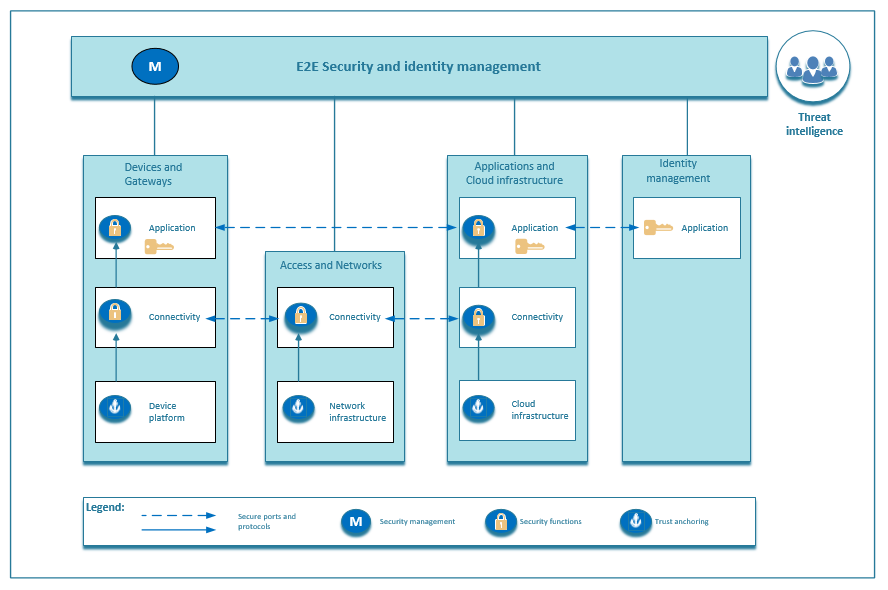


Figure 8 - E2E approach to security and identity management for the DIP.

## Domain security

Domains are built on trusted cloud resources and software. They include security and privacy functions to handle identity and access management, data protection, network security, logging, key and certificate management, and cloud infrastructure security.

Centralised management of security and identity functions within domains ensures that security and identities are properly managed, configured and monitored within the domain. Vulnerability and security baseline management also occur at the domain management layer.

### Navigating domain security

#### Horizontal

Inter-domain security is required at two levels: connectivity and application.

1. Depending on connectivity type, security controls such as mutual authentication and encryption of data in transit are provided at the connectivity level.
2. On top of connectivity, security is provided at the application level from Market Participants to the DIP, based on identification and access management functions and application security policies.
   * The Application level security can be independent of or dependent on (federated with) the connectivity level security.
   * Additional application-level encryption will not be implemented at this time.

#### Vertical

Intra domain security functions define Cloud infrastructure to applications and can be used in every domain to provide the necessary 'root of trust', thus ensuring the integrity of the domain. For example:

* Microsoft Trusted launch for Azure is available to provide ‘root of trust in the cloud.
* AWS NitroTPM, a Trusted Platform Module (TPM) 2.0 and Unified Extensible Firmware Interface (UEFI) Secure Boot support, can provide the root of trust in the cloud.
* The Cloud provider services (Azure, AWS, GCP) are accepted as the root of trust.

### Domain Communications (internal / external)

In order to maximise interoperability, interfaces and security functions should be designed to embrace open standards as much as possible. (Standards such as OIDC, SCIM, TLS, https etc.)

Standard security patterns (guardrails) define the (allowed) Ports and protocols supporting ALL;

* External communications.
* Internal communications
* Cross-Domain communications
* Inter-Domain communications.

### Domain Security functions

Security functions are deployed at the domain level based on standard security patterns (guardrails), which in turn define the security controls to be applied at a device and communications level.

* Security functions comprise standard security patterns (guardrails) and policies - baseline security configuration.
* Devices residing in a domainmust inherit the baseline security configurations for that domain.

All security configuration settings must be deployed as code such as ‘Terraform’ or configuration settings that are applied via policies held centrally in the cloud.

Changes to agreed security patterns (guardrails) and policies can potentially affect the integrity of the domain model or, in extreme cases, the entire security of the DIP. Therefore all requests for exceptions to security functions of a domain must be subject to a risk assessment and any required security testing (Penetration testing) undertaken.

## Asset management

Domain level security management requires an accurate asset inventory, including all the assets that must be protected in the domain (Cloud resources and software).

Automating asset discovery and continuous monitoring is essential to keep the asset inventory updated.

## Vulnerability, threat and risk management

Vulnerability information must be correlated with the asset inventory to monitor and remediate assets' vulnerabilities.

Rapid detection of attacks is crucial. Security monitoring and analytics functionalities must have the ability to analyse logs, events and data from the domain components combined with external data about threats and vulnerabilities.

Machine learning technology makes it possible to learn from and make predictions based on data.

* Coupling a machine learning analytics engine (UEBA or XDR, for example) with central threat intelligence improves the detection of zero-day attacks and reduces the response time for known threats.

On top of a monitoring and analytics engine, solutions relating to vulnerability, threat and risk management, along with security policy and orchestration components, are also required to automate security controls and maintain them at desired levels in a changing threat landscape.

Combining the information feeds for vulnerability, threat and risk management results in timely and accurate information for evaluating potential risks and helps direct efforts to protect the most exposed critical assets.

## Identity and access management

### Identity management

The main purpose of identity management is to manage the life cycle of identities and provide identification, authentication and access control services for identities. Various identities serve different purposes in the DIP, but the main ones are for device and user identification. Other accounts may be used for the management of devices, functions and services. Identifiers and keys are also used to sign and encrypt data, including software and firmware.

These different device identities are needed to identify the devices for connectivity within the ‘access and network’ domains and to identify device applications in the DIP ‘application and cloud infrastructure domain.

* The level of trust in the device identity depends on the strength of authentication both at the connectivity and application layers.
* Strong authentication and follow-up of the device integrity are needed for the device identity to be trusted.

#### Device identity

A device may have different identifiers depending on where it is in its life cycle. Life cycle management of device identities is part of the security management layer.

* The DIP system must authenticate the device, and newly given identifiers and credentials (bootstrap process) will be used for connectivity and application accesses.
* Connectivity identities are dependent on the connectivity type and have different life cycle management processes.

#### User identity

The user identities are needed to identify the users of the services within the application and cloud infrastructure domain. There may be several different ways to verify (authenticate) the user identities, such as single or multi-factor authentication, federated authentication, or authentication tokens. Each of these provides a certain level of authentication strength. Any identity and access management solution must be able to cooperate with and adapt to external identity and access management systems.

### Access control

On top of identification and authentication, users must also have access controlled so that only the permitted services are authorised.

Access controls are also applied to administrative functions performed by privileged users. They allow the configuration of privileges based on an administrative role and enable administrative functions without providing access to the actual data. Access can also be maintained on tables and schemas, providing further segregation of administrative duties. In addition, the identity and access management component provides the capability to manage and track administrative user access by issuing one-time passwords for administrative access.

Access control is applied at other layers of the architecture as well. When end users attempt to access data, their requests pass through several components that perform authentication and/or authorisation. For instance, the API gateway intercepts message requests in the network DMZ, handles user authentication, and supports single sign-on (SSO).

Applications, processes, and services may be configured to accept SSO tokens or require their own form of authentication.

The chosen identity and access management solution must also support.

* Privileged identity / privileged access management
* ‘Just in time’ access
* Role-Based Access Controls (RBAC)
* Least privilege

## Security patterns (guardrails)

Drafter’s note: to be defined in the DIP design phase.

## Compliance monitoring

Having the security baseline configuration and compliance function at the domain level ensures the automated hardening of the protected assets and supports continuous compliance monitoring in the defined security baseline.

* The solution must report on NIST, GDPR, ISO27001 and NCSC CAF compliance as a minimum.

## GDPR compliance

Data integrity, data confidentiality, accountability and privacy by design are all fundamental to protecting PII and consumption data. Such data can be protected via appropriate privacy controls. These controls include PII and consumption data and classification, personal data management and fair data processing practices.

When actual PII / consumption data might be exposed, additional privacy-protective measures, such as data encryption and data anonymisation, will need to be applied. Dedicated privacy logging and audit trail functionality can be used to improve the ability to predict, detect and respond to privacy breaches more promptly and flexibly.

* Such capabilities will be essential to respond to privacy breaches swiftly (within 72 hours, as prescribed by the GDPR). `
* Implementing GDPR compliance policies at the domain security layer makes it easier to meet GDPR requirements. The policies must provide identification and classification of PII and consumption data, enforcement of these privacy policies according to the GDPR, demonstration of compliance to the GDPR, and detection, response, and recovery from privacy incidents.

## Data loss prevention

Data loss prevention tools should be configured to work with the security management and automation solution, as highlighted in section 6.9 GDPR compliance.

## Response / Incident management

A high degree of automation is necessary to ensure a swift response to any identified threats and anomalies. Since not all security breaches and attacks can be prevented, it is crucial to have an efficient security incident management process that ensures rapid response and recovery. Real-time insights and audit trails from tools such as security monitoring, analytics and log management help to find the root cause of an incident. The same information can also be used as evidence in digital forensic investigations.

## End to End Security management and automation solution

The E2E security management and automation solution must provide unified security management across the DIP with adaptive prevention, detection, response, and security policy-driven compliance. This approach helps automate security and privacy controls, maintain them at the desired level even in a changing threat landscape, and shorten the reaction time in response to potential breaches.

The solution should provide real-time visibility of the security functions and patterns in order to remediate policy violations quickly and demonstrate compliance to GDPR, NCSC CAF and any custom MHHS security and privacy policies should they be required.

What the security management and automation solution must do:

* Evidence compliance to GDPR and the NCSC CAF.
* Provide industry standards-based security and policy-driven protection, helping to automate and maintain security policy and functions at the domain level, even in a changing threat landscape.
* Constantly monitor compliance of the security policies and functions, and provide threat and vulnerability detection to reduce the time from early detection to resolving potential incidents.
* Turn Data collected from the security management solution into powerful security insights, identifying relevant threats and vulnerabilities.

The orchestration layer unites predict, prevent, detect and respond, and transforms security from an event-driven architecture to a risk-driven adaptive security architecture. Figure 9 below illustrates a security management and automation solution.

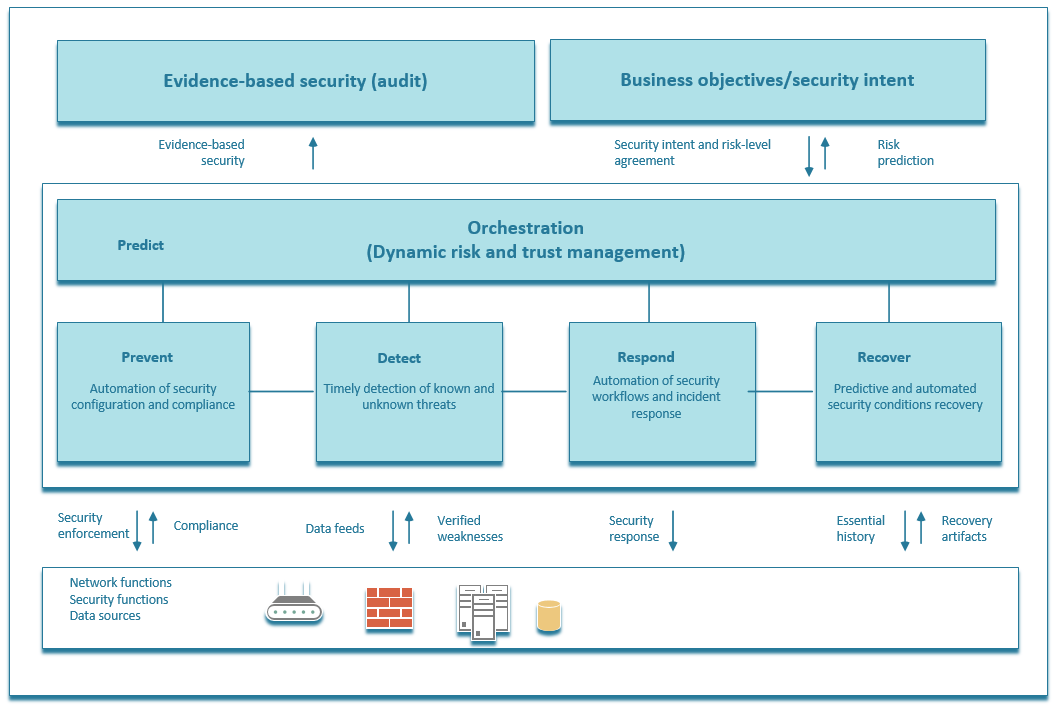


Figure 9 - Security management and automation solution**.**

# Deployment and operation of the security management solution.

## Provide cyber security services

The DIP Service Provider shall ensure a Cyber Security Programme (CSP) provides services through several key elements that focus on information sharing, advice and assistance. These elements aim to develop an intelligent, proactive approach to mitigating the security threat to the DIP.

If advice and assistance are required to support any part of the security functions of the DIP, the DIP Service Provider shall be available to assist in a variety of activities, such as risk mitigation, threat identification, or incident recovery.

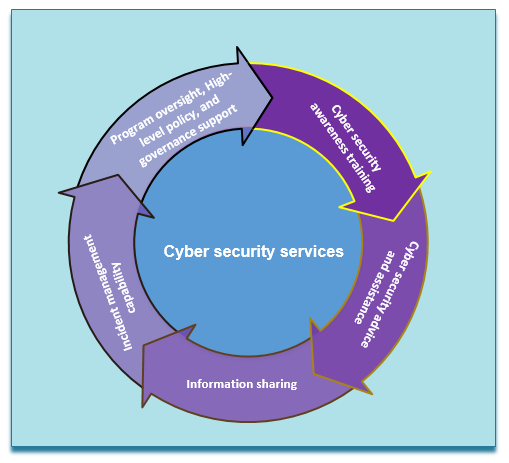


Figure 10 – Cyber security services

The DIP Service Provider shall ensure that the standards, patterns, policies and procedures provide sufficient flexibility to allow their adaptation across the DIP. In addition, achieving the goal of trusted data everywhere within the DIP requires partnerships and combined efforts with other components of the security community, Market Participants, service providers and any third parties to provide an integrated and adaptive systems security posture. Cyber security policies define the requirements and procedures required to effectively achieve the DIP's cyber-security goals.

1. Reduce the risk of loss, unauthorised disclosure, or unauthorised modification of the DIP, information assets and information systems.
2. Provide policy and guidance adaptable to meet the needs of the DIP and Market Participants aligned with the current threats.
3. Protect information by recognising and responding to threats, vulnerabilities, and deficiencies; ensuring that all systems and networks are capable of self-defence.
4. Establish and maintain a Cyber-Security Programme (CSP).
5. Document a System Security Plan (SSP) for each device.
6. Leverage research and development of advanced cyber security tools and capabilities within the energy industry.
7. Implement a DIP-wide Cyber Security training, education, and awareness programme.
8. Promote understanding and acceptance of cyber security principles throughout the DIP.
9. Maintain a DIP-wide near-real-time cyber security operational picture.
10. Implement integrated DIP asset management capability.
11. Implement DIP-wide cyber security services.
12. Achieve ISO27001 accreditation.
13. **Replace One-Time Security Gates with Context-Aware, Adaptive, and Programmable Security Platforms**

* Organisations need to replace the initial one-time, yes/no risk-based decision at the main gate to their systems (*typically managed by a static authentication and authorisation process*) with a continuous, real-time, adaptive risk and trust analysis of user anomalies with context-aware information across the platform. Context-aware security (also known as attribute-based access controls or ABAC) uses situational information, such as identity, geolocation, time of day, or endpoint device type.

1. **Continuously Discover, Monitor, Assess and Prioritise Risk — Proactively and Reactively**

* Risks events are fluid and require constant identification, analysis, prioritisation, monitoring, and response after the initial login assessment. This should include a combination of proactive and reactive capabilities. For example, if a user attempts to download a large amount of sensitive data, you need the ability to detect and prevent this action if it is considered inappropriate. Again, the use of ABAC can provide organisations with preventative controls at the business process, transaction, and master data level.

## Enable advanced cyber security capabilities

Agility in the security policies, guidance, and practices must be a goal for every process in the DIP. Continuous improvement is mandated.

The adaptive security approach places great importance on harvesting and prioritising ideas and the rapid development and deployment of concepts and capabilities to enable constant preparation, shaping, and execution of responses to the environment with tools such as;

* Security Orchestration, Automation and Response (SOAR), for example, Microsoft Sentinel or AWS Security hub.
* Advanced analytics and machine learning such as UEBA / XDR

The focus is to foster innovation and influence the planning and acquisition processes to further the cyber security posture and support the DIP as they may change.

## Develop a cyber-security empowered workforce

People are the foundation of good security practices and are also the greatest resource in protecting its information and systems. Establishing a comprehensive training, education, and awareness programme helps ensure that personnel understand their roles and responsibilities in protecting the DIP and its information assets, in preparing them to react to today's and tomorrow's threats. In today’s increasingly more capable and hostile threat environment, every employee plays an important role. The difference between being a vulnerability and being an element of defence-in-depth security can be measured in the quality of training, education, and awareness of employees.

Training, education, and awareness programmes also support the development of a professional workforce with the knowledge, skills, and abilities to prevent, deter, and respond to threats against the DIP’s assets.

Cyber security training, education, and awareness programmes provide critical management and operational support to the DIP's overall Cyber Security posture.

## Improve cyber security situational awareness

The complex and interdependent nature of the MHHS TOM and connectivity required to necessitate a shared cyber security awareness and understanding to enable effective operation. The DIP Service Provider requires sufficient visibility into the DIP’s resources to ensure the security protections applied are appropriate to protect, defend, and respond to threats.

To meet this need, the DIP Service Provider and Market Participants must work to identify situational awareness requirements and build and deploy a performance measurement capability to fulfil these requirements.

## Performance measurement:

The DIP Service Provider shall ensure performance measurements provide a clear and consistent way to measure success and demonstrate results. It helps to maintain a high-level overview of the current security posture by defining repeatable metrics and critical success factors. It ensures regulative, policy, and guidance requirements are being met and provides a feedback mechanism to adjust the DIP's cyber security programme and implementation, as needed.



Figure 11 – Performance Measurement

* Data Collection – Process for collecting and reporting cyber security metric information to the DIP Service Provider shall with the continuous status of the DIP's cyber security programme.
* Metrics Development – Process to develop and maintain the criteria for effective evaluation of the cyber security programme.
* Compliance and Monitoring Reviews – Process employed by DIP Service Provider to review compliance with established policy and guidance.
* Compliance Reporting – Establishes the process of delivering a standard set of reports that documents the DIP's current cyber security posture and status of its regulatory compliance milestones.
* Maturity Measurement – Process for evaluating all elements of the DIP's cyber security programme to identify the overall maturity of the programme elements and areas for process improvements.

1. Business Flows, Message Routing and Digital signing

Message Routing

Market participants will publish messages to the data integration platform (DIP) for onward routing to subscribers of those messages

* Table 3 below identifies which business flows require the message to be digitally signed or not, prior to forwarding to the DIP.

Digital Signing

Messages to be digitally signed.

The messages will be digitally signed, no encryption will be applied to the message:

* All data will be encrypted at the transport level using mTLS
* The Publisher digitally signs the message using private keys generated using the Certificate Signing Request (CSR) process with the DIP SP, which will be detailed in the MHHS PKI policy.
* The DIP verifies the message using the Publishers MHHS public key.
* The MHHS DIP signs the message using its Private Key.
* The recipient verifies the message data using the public key of the MHHS DIP.

Market Participants will never interact with another Market Participant to exchange certificate(s) / keys.

* All public certificates and keys will be managed individually between the MHHS DIP and the Market Participant.
* There will be NO shared keys using this pattern.

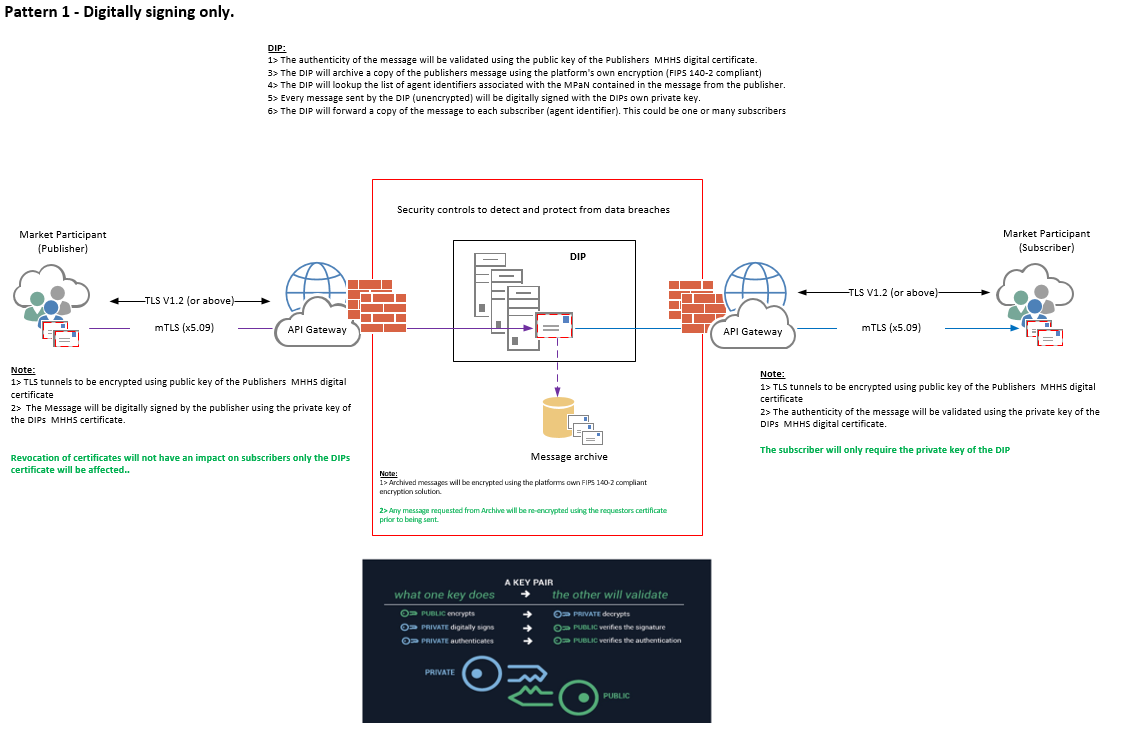
Drafter’s note: Table 3 below show examples of the business flows, the final business flows are TBD.

Business Flows

All messages contained within the business flows / interfaces will be digitally signed.

For an up to date list see MHHSP Interfaces Catalogue – IF\_LIST tab

Digital signing



1. End to End Security Requirements



1. MHHS AWG Security Principles and Data Architecture Standards





