CMAC CNS Technical Leaflet #10
Edition 28 April 2017

SWIM
System Wide Information Management

Civil-Military Reflections
EXECUTIVE SUMMARY

Recurring stakeholder and military questions on the emergence of SWIM require a guarantee that consumed/published information respects the relevant formats and quality of service levels. This includes not only the confidentiality, integrity and availability of information but also of attributes such as quality, liability and validity. Other issues include technical connectivity challenges as well as security and management/governance processes (who sets access privileges? who controls the interfaces/gateways? how is security managed? etc.).

Adherence to SWIM will likely offer enormous benefits to the military as it enables the enhanced sharing and harmonisation of data supporting advanced SES/SESAR concepts. SWIM envisages an “ATM intranet” whereby the ATM information held by the various system stakeholders is shared over a common platform.

SWIM is about building blocks that define middleware solutions and the information models and services to be supported. SWIM follows a number of principles including federated ownership of information, use of open standards to sustain semantic and technical interoperability, reliance on a service-oriented architecture (SOA) and service life cycle governance. Security is a fundamental attribute of SWIM.

The questions raised above must be addressed through an adequate level of military and stakeholders awareness on SWIM matters. Closer coordination of SWIM developments with military organisations is a must and relevant requirements, associated with information exchange needs supporting Air Traffic Management (ATM) and Air Defence, will be covered by SWIM-related research and deployment and standardisation initiatives. Military participation in SWIM governance structures is vital.
WHAT IS SWIM?

System Wide Information Management (SWIM) consists of standards, infrastructure and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services.

SWIM supports the ATM community with its need for timely, relevant, accurate, accredited and quality assured information. It enables the sharing of an integrated picture of the real-time and planned status of the ATM situation on a system-wide basis so that ATM operations are conducted safely and efficiently.

SWIM provides a common understanding of the different information domains in a network-centric environment interconnecting multiple domain systems that provide or consume information. Through SWIM, information is made available and processed on the basis of data models and services which need to conform to applicable standards and be registered.

In terms of technical infrastructure support, multiple stakeholders will be connected to SWIM, respecting specific profiles that are part of SWIM nodes and the service-oriented architecture (SOA). In a transitional phase, SWIM will facilitate information exchanges with legacy systems.

SWIM PRINCIPLES

SWIM is based on a number of fundamental principles including: 1) Federation – users collaborate in a federated manner at pan-European, regional and local levels; 2) Information-sharing - information will be available to a greater number of ATM stakeholders based on specific sharing policies; 3) SOA - SWIM will use services as the basic mechanism, decoupling producers of information from consumers in order to increase flexibility; 4) Open standards - SWIM services will be based on open and internationally agreed standards to the maximum extent possible; 5) Service life cycle governance - SWIM information, services and underpinning infrastructure specifications will be governed throughout their life cycle.

HOW TO BUILD SWIM?

SWIM is to be built on the basis of the following elements:

1) Standardised definitions of the information exchanged, e.g. conformance with the ATM Information Reference Model (AIRM) or existing standardised data exchange models;

2) Standardised description of Information Services, providing a common baseline on discovering, understanding and implementing Information Services;

3) Information Management Functions (including governance) - organisational functions for the management of user identities, discoverability of resources, security aspects such as confidentiality, integrity, non-repudiation, accountability and authenticity;

4) SWIM Technical Infrastructure (SWIM-TI) - interoperable infrastructure (ground/ground and air/ground) via which ATM information through services is distributed, shared and consumed.

These four elements enable the so-called SWIM-Enabled Applications – the ATM applications that publish or consume information services based on SWIM standards and principles, assuring the provision of commonly understood quality information.

By applying standardised information definitions, SWIM provides a common understanding of the different domains of information. Some specific data exchange models, mapped on the AIRM, have already been developed for specific information domain based exchanges: the aeronautical information exchange model (AIXM), which is already in use, the flight information exchange model (FIXM) and the weather information exchange model (WXXM) are good examples of this.
SWIM TECHNICAL INFRASTRUCTURE (SWIM-TI)

SWIM-TI is a set of software components distributed over a network infrastructure (middleware) providing capabilities properly enabling collaboration among ATM systems. These capabilities are instantiated in a set of SWIM nodes (stakeholder end points) and common components (providing capabilities to all the distributed SWIM nodes).

The SWIM node concept represents a package of SWIM-TI capabilities, allowing a given system to use the SWIM-TI. Examples of common components are the registry, which is used to enable the sharing of information (metadata) about services, or the public key infrastructure (PKI), aimed at managing the trusted digital certificates.

A SWIM Profile is a particular set of middleware functions/services tailored to meeting specific functional and non-functional requirements expressed in an Information Service Description. The latest definition is: “a SWIM profile is a coherent, appropriately-sized grouping of middleware functions/services for a given set of technical constraints/requirements that permit a set of stakeholders to share Information. It will also define the mandated open standards and technologies required to realize this coherent grouping of middleware functions/services.”

The SWIM Profiles identified in SESAR R&D include: Yellow Profile (initially developed for all exchanges with less demanding Quality of Service (QoS) requirements), Blue Profile (exclusively developed for real-time or near-real-time exchanges between ATC centre Flight Data Processing Systems), Purple Profile for Air-Ground SWIM and the Green Profile for specific civil-military requirements (if any). Only the Yellow Profile is considered to be mature for deployment and is currently the subject of further standardisation work.

Beneath the SWIM-TI middleware layer there needs to be an IP network infrastructure: IPv6 SWIM backbone, enabled by communication providers (e.g. PENS/NewPENS) or the use of B2B and B2C web interfaces.
The PCP Regulation\(^1\) introduced Initial SWIM requirements (ATM Framework \(^5\)\). Recent deployment initiatives revealed the willingness of multiple military organisations to actively pursue the deployment actions required to adhere to Initial SWIM.

Initial SWIM represents the first deployment steps, supporting information exchanges that are built on standards and delivered through an internet protocol (IP)-based network by SWIM-enabled systems. It comprises\(^2\): Common Infrastructure Components, SWIM Technical Infrastructure and Profiles as well as Aeronautical, Cooperative Network, Meteorological and Flight Information Exchanges.

### Common infrastructure components:

A number of common components/structures will need to be put in place by the operational stakeholders to facilitate SWIM interoperability and interconnectivity. This comprises Internet Protocol version 6 (IPv6), Pan European Network Services (PENS and NewPENS), SWIM governance, SWIM registry as well as Public Key Infrastructure (PKI) and cybersecurity measures.

### SWIM technical infrastructure (TI) and profiles:

Relying on standards and interoperable products and services, SWIM information exchange will be implemented on one of the following dedicated SWIM infrastructure (middleware) profiles: Blue SWIM TI Profile and the Yellow SWIM TI Profile. Blue SWIM TI Profile standardisation is currently delayed.

To become a SWIM subscriber, an infrastructure will need to be implemented including IPv6 networking as well as PKI and cybersecurity at local level. Availability of IPv6 will also enable compliance with Regulation (EU) 633/2007 on Flight Message Transfer Protocol (FMTP) (ATC-to-ATC coordination and transfer messages).

It is important to recognise that the stakeholder SWIM infrastructure evolution to comply with Initial SWIM requirements will also have to address stakeholder transition issues from legacy protocols to SWIM environment.

### Information exchanges:

The following information exchanges can be supported by Initial SWIM:

- Aeronautical Information - airspace reservation (ARES) data, D-NOTAM, airport data, AUP/UUP\(^3\) and other ASM and aeronautical data. Implementation must be compliant with the applicable version of the SWIM Specifications including the ATM Information Reference Model (AIRM).
- Meteorological Information (to be used in various contexts).
- Cooperative Network Information (ATFCM\(^4\) data, access to NOP\(^5\), and other NM-related exchanges).
- Flight Information (pre-tactical and tactical trajectory/flight object information for various operational purposes, including flight planning).

---

\(^1\) Commission Implementing Regulation (EU) No 716/2014 of 27 June 2014 on the establishment of the Pilot Common Project supporting the implementation of the European ATM Master Plan

\(^2\) iSWIM components targeted for deployment identified in EC Regulation 716/2014 of 27 June 2014 (PCP) – ATM Functionality \#5

\(^3\) Airspace Use Plan/Updated Use Plan

\(^4\) Air Traffic Flow and Capacity Management

\(^5\) Network Operations Portal
General considerations

It will be a national military prerogative to decide whether to rely on SWIM for any particular services on the basis of agreed information exchange requirements (IERs). When the military decide to adhere to SWIM, from a functional point of view it will be a normal SWIM participant. As a consequence, military users must respect the underlying SOA infrastructure and join on the basis of the defined standard interfaces in place.

IERs derived from operational scenarios reflect the role of military organisations as airspace users, ATC service providers, airport operators and command and control (C2) entities. Those IERs justify civil-military interoperability measures and contribute to military-military interoperability. Military ATM/C2 entities need comprehensive, accurate and timely flight/trajectory data on all flights currently within their area of responsibility (AoR). They also need access to aeronautical, meteorological, surveillance, and flow and capacity data relating to airspace and aerodromes within that AoR. Civil ATM entities need early sharing of planning information to improve CDM and the situational awareness of all military aerial activity. Access to military surveillance capabilities may be essential in order to maintain coverage of the relevant AoR.

Data formats and models

Prior to defining any interconnection approaches, an exhaustive assessment is needed in respect to the overall compliance of military systems or information with the current versions of aeronautical information and flight data standards, data quality requirements and communication protocols, including regulatory material included in SES Regulations and related Specifications.

Connectivity to SWIM-TI

Military users should respect the underlying SOA infrastructure and adhere to SWIM on the basis of defined standard interfaces (profiles) in place. Based on the applicable QoS requirements (including availability) the appropriate profile colour must be chosen. Yellow Profile will likely meet the availability requirement in almost all cases. This can mitigate the fact that Blue Profile is not yet fully mature to support operational critical flight data (e.g. flight object). The Yellow Profile is based on the Web Services stack of standards running preferably over IPv6 and can be made sufficiently secure using Virtual Private Network (VPN) tunnelling. Purple and Green Profiles are still under research (SESAR 2020). The military must influence the research work on Green Profile so that any particular military requirements are adequately considered.

The new SWIM TI Green Profile must take due account of the legacy protocols used by military systems, specific security requirements as well as already developed profiles. Military Organisations might decide to seek proprietary/local interoperability options outside the context of SWIM.
Interfaces

Military ATM and Air Defence/C2 system connectivity with the underlying SWIM architecture depends heavily on the efforts to define and validate specific interfaces (being researched in SESAR 2020).

Such interfaces should allow data exchange between the networks of different security domains. In the case of SWIM, they would also enable communication with military legacy systems where information exchange requirements so justify.

SESAR 2020 efforts are expected to completely define and validate an interface model, including at the middleware level (Green Profile), and physical network level. Such interfaces need to take into account all possible alternatives for the military to connect to SWIM, depending on the services supported and local conditions. This interfacing definition must start from the description of specific military protocols to delineate potential encapsulation strategies.

SWIM IP backbone

Potential military ATM and Air Defence/C2 system connectivity with underlying SWIM structures might entail the adherence to a NewPENS IPv6 SWIM backbone, enabled by communication providers, or the use of B2B and B2C web interfaces, particularly when the client applications supported are not operationally critical.

Security

The military might agree to connect their systems to SWIM if two conditions are met. Firstly, if the military are able to apply their own security policy (generally based on their own safeguard mechanisms and measures). Secondly, if the military are involved in the definition of overall SWIM security policy and have confidence in its enforcement.

Military adherence to SWIM may require security issues to be addressed. The main four security topics are the following:

1) Penetration (protection against unauthorised access) - The military will need assurances that their systems will not be exposed to the risk of intrusion via the SWIM node;

2) Confidentiality - The military may publish unclassified information which might still be sensitive in some situations. Assurances about non-disclosure will be needed;

3) Data Integrity - Data integrity provisions protect information against unauthorised modification. A military SWIM node needs to be able to verify the integrity of the information received;

4) Availability - A high level of availability is needed to protect military systems against denial of service attacks.

Without prejudice to internal SWIM security measures, the overall definition, accreditation and management of security mechanisms and practices associated with a node interconnecting a military system to SWIM must remain primarily under the ownership and supervision of military authorities.

Military participation in SWIM might entail additional specific requirements in terms of security levels adequate for the information shared by military organisations. Use of PKI and Cybersecurity services can contribute to achieving defined levels of security in terms of emission/revocation of certificates and security of information transfer.
**SWIM governance**

If the military decide to use SWIM, it is essential that they actively participate in SWIM governance, i.e. the bodies and processes that coordinate the operation of SWIM and its controlled evolution. SWIM governance is of utmost importance for military organisations, both procurement agencies and armed forces, as it should be the key organisational structure for coordinating the evolution of SWIM in order to ensure civil-military data exchange interoperability.

**SWIM standardisation**

The European ATM Standardisation Coordination Group (EASCG) concluded that a number of recognised standardisation bodies should support the European implementation of initial System Wide Information Management (iSWIM) by making available a number of appropriate standards as identified in Commission Implementing Regulation (EU) No 716/2014 on the establishment of the Pilot Common Project supporting implementation of the European Air Traffic Management Master Plan.

Three standardisation bodies, EUROCAE, CEN and EUROCONTROL, were identified by the EASCG to provide technical specifications for three distinct standardisation areas supporting iSWIM implementation: 1) Foundational Information Service Description, Information Definitions and Yellow Profile Technical Infrastructure specifications coordinated by EUROCONTROL. 2) ATM information security specifications, coordinated by CEN - an amendment of the Standard on information security for organisations supporting civil aviation operations (EN 16495:2014) is anticipated. 3) Specific information exchange service implementation specifications, such as "Arrival Management Information Service", coordinated by EUROCAE through working group 104 (WG-104).

Military organisations will be encouraged to actively take part in that SWIM Standardisation process.

**Plan to migrate towards SWIM**

When planning interoperability initiatives for SWIM connectivity, military organisations may consider:

- Extensive reliance on AIXM to enable systems to exchange aeronautical information in the form of XML encoded data. It will enable dynamic context based on the retrieval/delivery of aeronautical Information as opposed to the current semi-automated AIS

- Flight data management fully based on UML-driven Flight Object concepts to allow disparate systems from different suppliers, from within different organisations with different viewpoints, to share information

- Trajectory Management functions that will play a major role in future ATM concepts

- Using appropriate protocols defined in the SWIM technical Infrastructure Profiles. The SWIM TI Yellow Profile is available to support immediate implementation initiatives

- Contributing to SESAR 2020 to define and validate a new SWIM TI Green Profile which will take due account of the legacy protocols used by military systems as well as specific security requirements

- Benefitting from the widespread use of B2B and B2C web interfaces that will support a wide range of client applications, namely those that are not operationally critical

- Accessing to Internet Protocol version 6 networking, e.g. subscription to NewPENS IPv6 services as the means to access the SWIM IP backbone

- Implementing IPv6 at local level where ATM information needs to flow to/from civil domains

- Seeking proprietary/local interoperability options outside the context of Initial SWIM, where appropriate

- Security measures like Public Key Infrastructure and Cybersecurity

- Military participation in SWIM governance processes

- Contributing to SWIM Standardisation

---

7 Members: EC DG MOVE, EASA, SJU, EUROCAE, CEN/CENELEC, ETSI, EUROCONTROL; and Observers: SDM, EDA, ASD, CANSO
Overall, SWIM solutions will be further developed in the framework of ICAO, SESAR and other activities to consolidate concepts and to further validate and demonstrate their suitability in multiple other domains such as SWIM TI Profile maturity, security and governance.

The benefits for military organisations and for European ATM Network (EATMN) as a whole from military adherence to SWIM depend on the ability to seamlessly exchange information between civil and military systems, enabling CDM and enhanced coordination as a whole and contributing directly to higher levels of ATM performance and efficiency.

In particular, the exchange of data between civil and military systems in a net-centric context can enable trajectory concepts, use of advanced Flight Data Processing System (FDPS) functionalities, enhanced airspace planning and management process, use of high quality static and dynamic ATM data, improved air picture for ATC and Air Defence purposes, lower coordination overheads, tracker and sensor rationalisation and response to security concerns.

The benefits offered by SWIM to the military can be summarised as follows:

- Seamless civil-military information exchange.
  Net centricity. CDM. Security
- Implementation of trajectory and other SESAR concepts
- Use of advanced FDPS
- Enhanced ASM planning and management
- Use of high-quality/harmonised ATM data
Authors:
Jorge PEREIRA
Head of Unit DATM/CMC/CNS
Dominique GUILLERM
Data Processing Expert DATM/CMC/CNS