# Learn to SWIM

Matias Krempel
Deutsche Flugsicherung, Langen, Germany

Martin Gilje Jaatun
SINTEF ICT, Trondheim, Norway

***Abstract*—This paper is meant to provide an overview over SWIM and its context from a security point of view. Rather than describing everything in detail it refers to the relevant SJU deliverables where possible and tries to provide the "glue" between the different pieces of information.**

***Index Terms*—SWIM; SESAR; SJU; ATM Security; MSSC;**

## I. Introduction

System Wide Information Management (SWIM) is a service concept meant to improve information sharing in future Air Traffic management. It will gradually replace most legacy information exchanges, although some (currently for instance surveillance data) are not planned to be exchanged through SWIM. Critical data exchanges from/to aircraft, especially clearances, will still be made using legacy datalink (CPDLC, ADC-C).

The concept of SWIM is accepted at the global level as an element in the ICAO Aviation System Block Upgrades (ASBU) [1]. This framework represents the global consensus on ATM solutions or upgrades from the implementations plans in many regions of the world. like Single European Sky ATM Research (SESAR) in Europe, NextGen in the US and CARATS in Japan. The SWIM concept predates SESAR, as documented in the EU FP6 project SWIM-SUIT [2]. There are currently 3 SWIM TI prototypes being developed in SESAR, and used in validation exercises, for instance to validate i4D exercises (SWIM ground-ground), or exchanges of meteo data or aeronautical data. These prototypes will include some (not all) of the security controls specified for SWIM in SESAR.

## II. SWIM in SESAR

In SESAR the overall picture of ATM is documented in the European ATM Architecture (EATMA). The underlying architecture model follows the NATO architecture framework. It provides different views of SESAR operational improvements.

According to the SWIM Concept of Operations SWIM consists of standards, infrastructure and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services. It features the following elements:

- an ATM information model (AIRM) representing the standard definition of all ATM information, through harmonised conceptual and logical data models. In the context of the SESAR Programme, this is instantiated in the AIRM (ATM Information Reference Model). AIRM takes into account new standards for ATM data such as AIXM-5 for aeronautical data for instance.
- an ATM services model (ISRM) representing the logical breakdown of required information services and their behavioural patterns. These services could also be described as ATM-specific services. In the context of the SESAR Programme, this is instantiated in the ISRM (Information Service Reference Model);
- information management functions, such as operational and organisational functions for the management of user identities, discoverability of resources, security aspects such as authentication, encryption and authorisation, notification services and registration. These functions need to be defined to support information sharing. The SWIM governance functions affect almost all of the roles and their interactions within the European ATM system [3];
- the SWIM technical infrastructure (SWIM-TI),which is the interoperable (runtime) infrastructure (ground/ground and air/ground) via which ATM data and services are distributed, shared and consumed. Its implementation may, depending on the specific needs profile, differ from one stakeholder to another, in terms of both the scope and the type of implementation. It will mostly be based on commercial off-the-shelf (COTS) standards-based and interoperable products and services, but it is possible that in some cases specific software may need to be developed;
- SWIM-enabled applications: the application of SWIM standards and principles to the interfaces of ATM applications enables ATM business benefits by assuring the provision of commonly understood quality information to the right people at the right time.

SWIM services, their interfaces and functions can be found in the Service Layer of EATMA. Several other services are being defined and will be integrated further. SWIM services deal with information elements described in the AIRM and the information exchanges, both elements are part of the operational layer of the EATMA. Information elements are detailed in information entities. The SWIM services follow a taxonomy and are structured via governance of SJUs service coordination group (SCG).

SWIM has its own "sub" architecture which is described in the SWIM Architecture Principles [4]. This document also describes the links to the EATMA views.

SWIM is developed in iterations, which are aligned with the storyboard 3 steps of SESAR:

1) Time based operations
2) Trajectory based operations

3) Performance based operations

The current focus of the SESAR SWIM WP is to support the enhancements which are part of the Pilot Common Projects (PCP) to be approved by the European Commission, which are foreseen to implement an initial subset of the SESAR results.

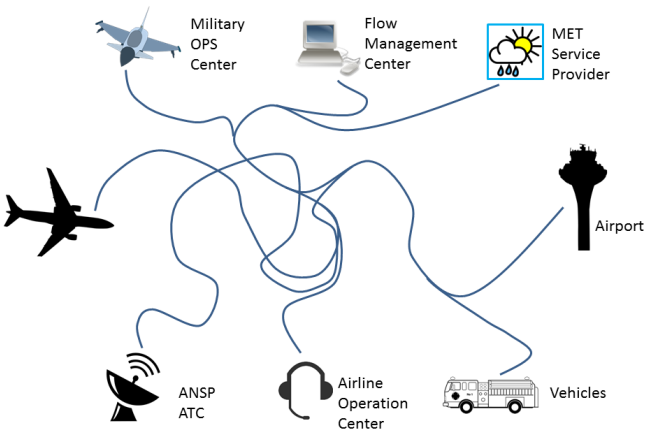


Fig. 1: Aviation communication before SWIM [5]

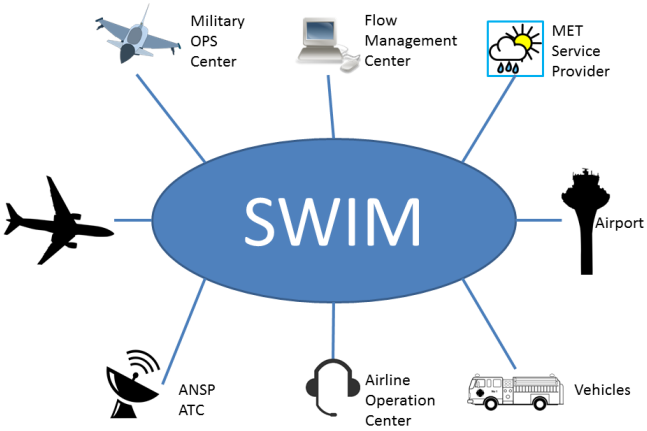


Fig. 2: Aviation communication after SWIM [5]

### A. SWIM Technical infrastructure

The technical infrastructure is described in the SWIM-TI Technical Specification. It is important to note that this is a functional architecture, as the purpose of SWIM design is to define only the minimal elements that will enable SWIM TI implementations to interoperate. The SWIM TI is subdivided in functional blocks which are either part of SWIM nodes or common components according to the following structure:

- SWIM nodes
  - Policy enforcement point - PEP
  - Messaging - MSG
  - Data Validation - DV
  - Security - SEC
  - Local Supervision - SPV
  - Recording - REC
  - High Availability - HA
  - Shared Object - SO
- Common components (also named “shared functional blocks” and “common functional blocks”
  - Registry - REG
  - Public Key Infrastructure - PKI
  - Bridge Certification Authority - BCA

SWIM services use subsets of the capabilities of the functional bocks. These “capability subsets” are standardized into profiles.

### B. Security in SWIM

The overall approach to security in SWIM is presented in Fig. 3.

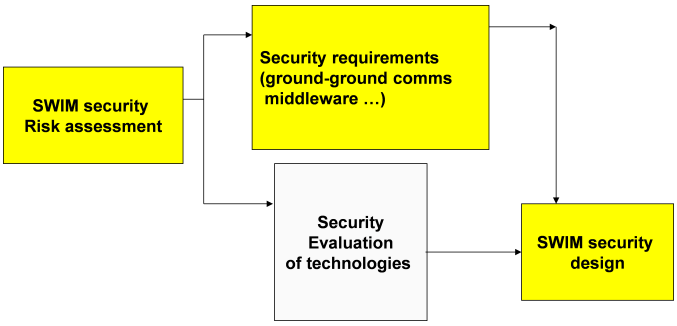


Fig. 3: Overall approach to SWIM security

Security requirements form part of the overall set of requirements [5]. Requirements produced by Project 14.2.2 are detailed in Project 14.1.4 (Interface specifications and Services Technical requirements). The requirements are maintained in a central requirement repository based on DOORS [1] Security requirements would – by “schoolbook wisdom” – have to come from two sources:

- A set of high level requirements derived from general consensus on security best practices called Minimum Set of Security Controls (MSSCs) and
- the results of security risk assessments described in the following paragraphs in terms of
  - additional controls rsp.
  - proof that certain MSSCs are not applicable

Such high level requirements will then have to be detailed and fed into the design.

In practice, work on SWIM had to start before SESARs security reference material was available / mature. This required Project 14.1.4 to add security aspects to the SWIM-TI Technical Specification documentation and Project 14.2.2 to

[1] http://www-03.ibm.com/software/products/en/ratidoor/

add security requirements to their overall requirements in the SWIM design papers [5] based on own research.

These existing security requirements from the design papers have to be related to the respective MSSC list as soon as the MSSCs are available and to the control requirements derived from the security risk assessments. The 14.02.02 project complements the high-level MSSC requirements by more detailed controls taken from existing standards, such as ISO/IEC 27002 [6] and the NIST standards family. This is mandatory work to enable specification of precise requirements in the SWIM technical specification. This work will be fed back to the MSSCs.

### C. Security in SWIM TI

In the SWIM-TI Technical Specification, security is primarily addressed in the SWIM-TI functional block "Security" and the "safety & security" paragraph of all functional blocks. However, there are also requirements which specify controls in almost every part of the technical specification, such as the ones in monitoring or data validation, for instance. The functional block Security provides Confidentiality, Integrity, Authentication, Authorization and Audit functionalities, allowing data exchanged through the SWIM-TI to be protected. An overview picture derived from the SWIM TI Technical specification can be found in Fig. 4.

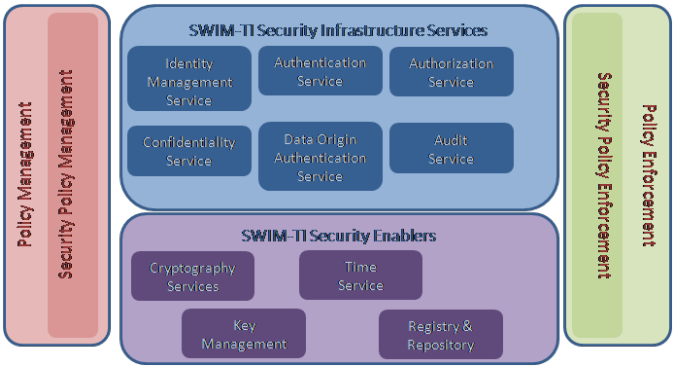


Fig. 4: Overview of the SWIM TI Technical Specification

Key Management relates to the PKI functional block which – in turn – relates to the BCA functional block, which facilitates mututal trust between different PKI hierarchies.

## III. SWIM Security and Transversal SESAR ATM Security

ATM Security is concerned with limiting the effects of unlawful interference (i.e., deliberate acts) on the ATM function and providing outside agencies (law enforcement, military agencies, emergency services or incident investigation agencies) with support during an incident [7]. SWIM security is thus an important part of ATM security.

SESAR ATM security will have to address both the final operations of the Operational Focus Area (OFA) and the transition from today to final operations (i.e., the full system life cycle). Note that SWIM is not considered an OFA in itself, but rather an *enabler* needed by several OFAs. Examples of OFAs include *Queue Management in TMA and En-route* and *Airport Operations Management*.

It addresses the following impact areas

- IA1:PERSONNEL
- IA2:CAPACITY
- IA3:PERFORMANCE
- IA4:ECONOMIC
- IA5:BRANDING
- IA6:REGULATORY
- IA7:ENVIRONMENT

In order to address the following categories for controls, SWIM will deliver security requirements and evidence to develop a security case.

The OFA Security deliverables shall include

- the SJU ATM security policy;
- a security concept containing
  - participation in collaborative support during the deployment and implementation phase;
  - describe what is to be protected and the goals of IPOCM within the OFA during the deployment and implementation phase;
  - alignment with with any SESAR security concept;
  - roles and responsibilities of all the OFA/Primary Project team and security experts. In addition to the OFA roles, there may be external actors, such as suppliers or developers who may have an impact on the security of the OFA;
  - definition of security of all elements in the OFA In addition to the policy elements, there may be additional elements such as external equipment, interfacing with external actors such as the military;
  - consideration of the OFA role as part of SESAR and ATM in general.
  - Definition of Validation objectives for the collaborative support and self protection concepts.
- enabling collaborative support;
- ensuring the resilience of the system;
  This will have to include the development of Incident Preparedness and Operational Continuity Management (IPOCM) functional and performance requirements based on the IPOCM concept.
- coordinating security with other elements of ATM, providing evidence of
  - coordination and dependencies with other OFAs or outside elements in collaborative support and self protection have been identified;
  - requirements for the coordination of security have been generated based on the dependences with other OFAs or outside elements;
  - validation scenarios and exercise have been coordinated between OFAs and outside elements;
  - coordination has been successfully achieved.

The security risk assessment shall include

- a set of primary assets;

- the impact of unlawful interference for each SESAR KPA if the primary assets are compromised;
- the supporting assets;
- threat scenarios, based on threats to supporting assets from an understanding of their vulnerabilities;
- the likelihood of the threat scenario resulting in a successful attack on a supporting asset;
- the risk (a function of likelihood and impact);
- a set of controls to reduce the risk to an acceptable level.

The method applied for risk assessment in SESAR follows the standard ISO/IEC 27005 [8]. It is derived from earlier work by EUROCONTROLs Security Expert Team (SET). While the method is meant to be applied in the SJU it has to be noted that for the later phases of the system life cycle – notably industrialization, deployment and operation – other methods for risk assessments have to be applied based on national rsp. regional regulation [2]. This will probably require a refinement and rework of the high level risk assessments in SESAR.

For the sake of the SJU development phase, the level of detail of security risk assessment has been limited in the following way

- SWIM services defined in the ISRM documents are regarded as "level 1" primary assets.
- Supporting assets to the SWIM services address on the one side hardware, operating systems, interfaces and actors (humans) an on the other side the SWIM functional blocks as SWIM middleware. The SWIM middleware is assessed as two "black boxes" where one contrains the SWIM node based blocks and the other the common components.
- These supporting assets includeing the functional blocks are then assessed in term of vulnerabilities and threats that might apply.

EN 16495 [9] provides guidance on how to ensure interoperability of the results of different risk assessments done for different (SWIM) elements by different organizations.

The application of the risk assessment method comes with a couple of challenges. In general, the security reference material lacks a comprehensive list of threats, threat agents and vulnerabilities relevant for ATM domain. This has to be developed by the different OFAs.

This weakness seems to be systematic as these three elements are pretty dynamic by nature so that a consensus regarding stable structures needed for long-term high-level assessments is seemingly not available today. Furthermore, the determination of likelihood is expecially difficult to determine for long-term risk assessments. This is notably true due to the dynamic nature of credible threat agents and their motivation, and threat actions exploring vulnerabilities.

In SWIM we also have to consider that it is an enabler for the business services addressed in the European ATM architecture. This means that in theory it doesnt own a criticality by itself, but that the criticality of SWIM services is derived from the criticality of the services for their users. Within SESAR they are represented by the different OFAs. However, beyond SESAR other types of users might need to be considered for input to criticality assessments as well. While security requirements form part of the overall requirements, they need to be included in validation and verification excercises with the different business services, usually performed in the context of an OFA.

In practice the instable situation of the "SWIM customer" side needs to be alleviated by the definition of assumptions. These assumptions need to be validated through review by stakeholders. A higher involvement of stakeholders would ease the risk assessment work.

A security case will be developed by WP 16.6.2 based on the input provided by the OFA, according to the flow diagram depicted in Fig. 5. A security case is analogous to the more well-known *safety case*; the former represents a collected set of evidence that in total supports a claim that the system meets the criteria of a given security level. The security case may, however not be the final word, as there frequently are tradeoffs to be made due to conflicts between, e.g., safety, security and/or operational needs. The security case builds a comprehensive picture, but is only an input to the business case; perfect security is generally neither attainable nor affordable.

## IV. Transversal aspects

While all architectural information eventually ends in the EATMA repository, which is based on a tool called MEGA, the SWIM architects use for the documentation of their sub model a tool called Enterprise Architect (EA) whose results end in a local file. A free reader is available to browse this artefact. A synchronization is foreseen between the MEGA and the EA

From a security point of view SWIM services represent "Primary Assets" and as such are expected to be documented in SP 16.6.2s security repository.

## V. Conclusion

We believe that SWIM is the future of the European ATM landscape, but while this is just a first step on a core component, the complexity of implementation will put an extra challenge on the next step, and pragmatic tradeoffs in the years to come may lead to a SWIM system that is significantly different from the one we envision today. Nevertheless, SWIM will inevitably represent a backbone to security provision within tomorrow's ATM system.

## Acknowledgements

This paper is the result of collaborative research co-funded by the SESAR Joint Undertaking. However, the paper does not purport to represent the views of SESAR JU or any SESAR partner.

[2] See, e.g., EBIOS in France, MAGERIT in Spain and Italy, and NIST standards in the US

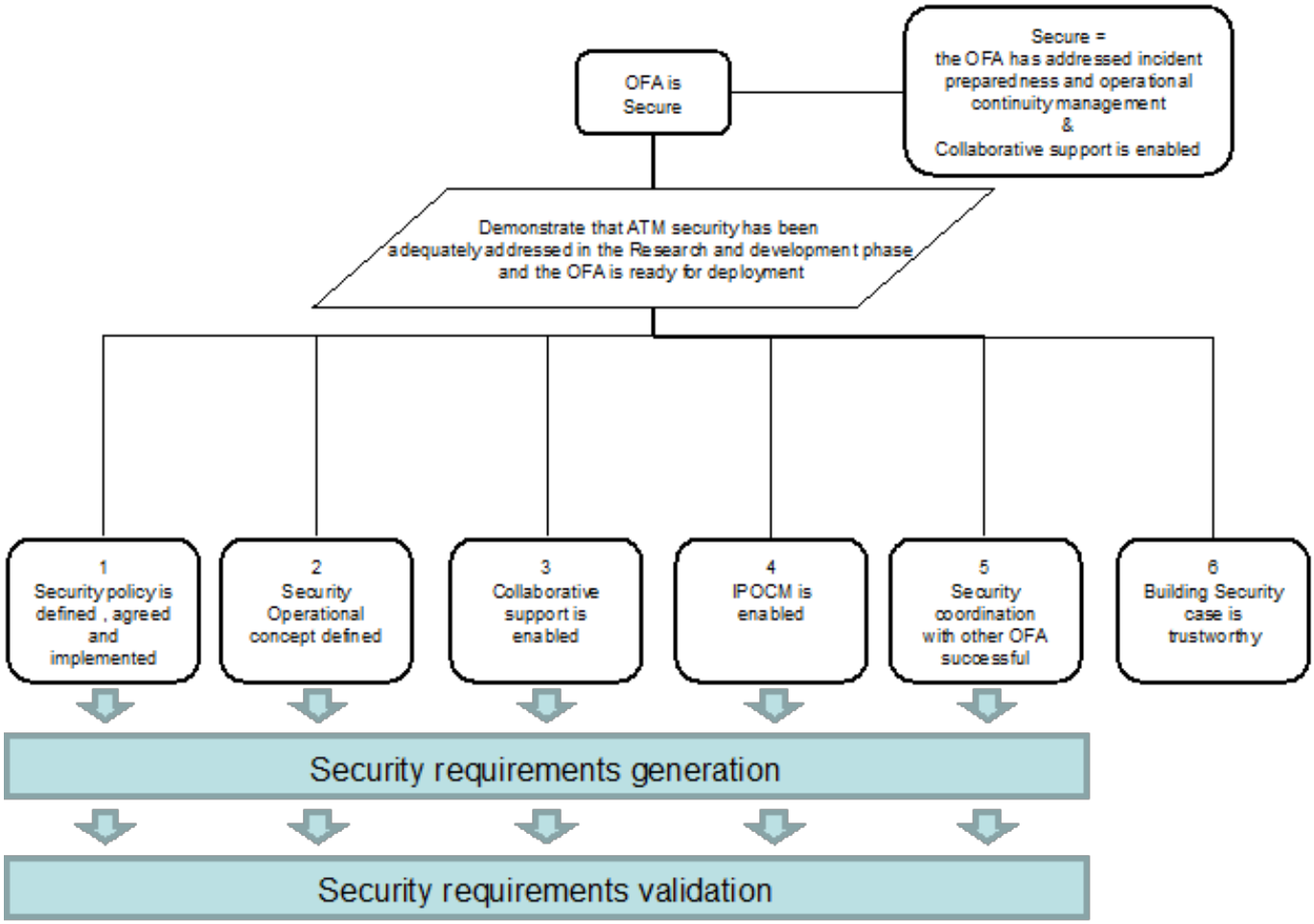


Fig. 5: SESAR security case

## REFERENCES


[1] Aviation System Block Upgrades . [Online]. Available: http://www.icao.int/Meetings/anconf12/Pages/Aviation-System-Block-Upgrades.aspx

[2] P. Fantappié, D. Smith, N. Silvester-Thorne, G. Bogdos, B. Badanik, A. Kazda, K. Havel, D. Scarlatti, and R. Schreiner, "SWIM-SUIT Security Requirements," 2008. [Online]. Available: http://www.swim-suit.aero/swimsuit/projdoc2.php?action=download&id=56

[3] P. Cruellas and E. Roelants, "SWIM Concept of Operations," 2013, 08.01.01 Deliverable D41. [Online]. Available: https://www.eurocontrol.int/sites/default/files/publication/files/del08.01.01-d41-swim_conops.pdf

[4] "SWIM Architecture Principles," 2013, 14.01.03 Deliverable D03.

[5] M. G. Jaatun and T. E. Fægri, "Sink or SWIM: Information Security Requirements in the Sky," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, Sept 2013, pp. 794–801.

[6] *Information technology - Security techniques - Code of practice for information security management*, ISO/IEC Std. 27002, Std., 2005.

[7] J. Hird and C. Machin, "SESAR ATM Security Reference Material - Level 2 - 2013," 2013, 16.06.02 Deliverable D101.

[8] *Information technology - Security techniques - Information security risk management*, ISO/IEC Std. 27005, Std., 2011.

[9] *Air Traffic Management – Information security for organisations supporting civil aviation operations*, EN Std. 16495, 2014.