ANIKETOS

Secure and Trustworthy Composite Services

SEVENTH FRAMEWORK PROGRAMME

Seventh Framework Programme:
Call FP7-ICT-2009-5
Priority 1.4 Trustworthy ICT
Integrated Project

Deliverable ID: D6.1	Preparation date: 19th July 2011

Milestone: Released

Title:

Initial analysis of the industrial case studies

Editor/Lead beneficiary (name/partner):
Paolo Pucci/ELSAG

Internally reviewed by (name/partner):
Paolo Giorgini/UNITN

Approved by:
Executive Board

Abstract:

Aniketos is about establishing and maintaining trustworthiness and secure behaviour in a constantly changing service environment. The project aligns existing and develops new technology, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service end users.

This deliverable provides an initial analysis of the three industrial case studies selected within the following areas: future telecommunication services, the emerging European Air Management systems, land-buying and e-Governance.

The case studies are described in terms user stories description, technology domains, domain specific requirements and security issues.

The analysis carried out in this document will guide the realization of the case studies.

Dissemination level		
PU	Public	X
CO	Confidential, only for members of the consortium (including Commission Services)	

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257930.

Aniketos consortium

Aniketos (Contract No. FP7-257930) is an Integrated Project (IP) within the 7th Framework Programme, Call 5, Priority 1.4 (Trustworthy ICT). The consortium members are:

SINTEF ICT (SINTEF) NO-7465 Trondheim Norway www.sintef.com	**Project manager:** Richard T. Sanders richard.sanders@sintef.no +47 73 59 30 06 **Technical manager:** Per Håkon Meland per.h.meland@sintef.no +47 73 59 29 41
Tecnalia Research & Innovation (TECNALIA) E-20009 Donostia - San Sebastian Gipuzkoa (Spain) www.tecnalia.com/en	Contact: Erkuden Rios Velasco erkuden.rios@tecnalia.com
Consiglio Nazionale delle Ricerche (CNR) 00185 Roma, Italy www.cnr.it	Contact: Fabio Martinelli Fabio.Martinelli@iit.cnr.it
Thales Services SAS (THALES) 78140 Velizy-Villacoublay, France www.thalesgroup.com	Contact: Dhouha Ayed dhouha.ayed@thalesgroup.com
Liverpool John Moores University (LJMU) Liverpool, L3 5UX, United Kingdom www.ljmu.ac.uk/cmp	Contact: Madjid Merabti m.merabti@ljmu.ac.uk
Selex Elsag S.P.A. (ELSAG) 16154 Genova, Italy www.selexelsag.com	Contact: Pucci Paolo Paolo.Pucci@selexelsag.com
SEARCH-LAB Ltd. (SEARCH) Budapest 1117, Hungary www.search-lab.hu	Contact: Zoltán Hornák zoltan.hornak@search-lab.hu
Atos Origin (ATOS) 28037 Madrid, Spain www.atc.gr	Contact: Pedro Soria-Rodriguez pedro.soria@atosresearch.eu

Telecommunication Software and Systems Group (TSSG) Waterford, Ireland www.tssg.org	Contact: Miguel Ponce de Leon miguelpdl@tssg.org
Universita Degli Studi di Trento (UNITN) 38100 Trento, Italy www.unitn.it	Contact: Paolo Giorgini paolo.giorgini@unitn.it
Athens Technology Center SA (ATC) 15233 Athens, Greece www.atc.gr	Contact: Vasilis Tountopoulos v.tountopoulos@atc.gr
SAP AG (SAP) 69190 Walldorf, Germany www.sap.com/research	Contact: Achim Brucker achim.brucker@sap.com
ITALTEL S.P.A. (ITALTEL) 20019 Settimo Milanese, Italy www.italtel.it	Contact: Maurizio Pignolo maurizio.pignolo@italtel.it
Paris Lodron Universität Salzburg (PLUS) 5020 Salzburg, Austria www.uni-salzburg.at	Contact: Manfred Tscheligi manfred.tscheligi@sbg.ac.at
Deep Blue SRL (DBL) 00193 Roma, Italy www.dblue.it	Contact: Valentino Meduri valentino.meduri@dblue.it
Wind Telecomunicazioni S.P.A. (WIND) 00148 Roma, Italy www.wind.it	Contact: Rita Spada MariaRita.Spada@mail.wind.it
Dimos Athinaion Epicheirisi Michanografisis (DAEM) 10438 Athens, Greece www.daem.gr	Contact: Ira Giannakoudaki i.giannakoudaki@daem.gr

Table of contents

List of figures

List of tables

Executive summary

This deliverable provides an analysis of the three industrial case studies selected. They are real-life cases where emerging composite services are expected to be relevant, thus they could benefit from the practical application of Aniketos results. In particular, Aniketos will help establish and maintain trustworthiness and secure behaviour in a constantly changing service environment. The selected case studies will show which methods could be provided for analysing, solving, and sharing information on mitigation of threats and vulnerabilities.

Case study A deals with enhanced telecommunication services in the Future Internet. It focuses on the possible evolutions of the telecom (TLC) operators' role. In order to face competition with the Web Service Providers, TLC operators are considering an open-platform business model in order to provide services which are exposed and consumed by using Web 2.0 service technologies, i.e. the so-called Telco 2.0 approach. Aniketos platform will offer TLC operators design time and runtime support for a secure and trustworthy service composition.

In order to improve end user experience in accessing these services, the realization of this case study foresees the usage of a Federated Identity Management system.

The reference network architecture is the NGN, as telecom operators are migrating to fully Internet enables network.

Case study B deals with the emerging European ATM systems that will result from the introduction of SWIM, the new interoperable middleware. SWIM replaces data level interoperability and closely coupled interfaces with an open, flexible, modular and secure data architecture. The openness of the information systems makes them vulnerable not only to malicious exploitations but also to integrity, confidentiality and availability risks. Furthermore trust problems arise between ATM stakeholders, who have to rely on mediated information. Aniketos will be able to address these security-related challenges.

Since SWIM case study is very complex it is restricted to design-time validation As a consequence it will be very demanding on the Aniketos design-time tools, especially the socio-technical modelling language.

The focus of the ATM/SWIM case study for Aniketos is on the governance in a system of systems environment and on core business services.

Case study C deals with land-buying and e-Governance. It represents a typical public service for searching a lot, buying a lot and issuing a house building permit. These kinds of services are becoming more and more available online, and need to address the key challenges identified for Aniketos project.

This application domain involves multiple potential stakeholders, ranging from ordinary citizens to various organisations from different domains. This case study involves many factors affecting decisions at various stages and many security threats and vulnerabilities that Aniketos platform support will help to face.

The target outcome will be to facilitate access to the most up-to-date procedures, information on relevant regulations and advice on associated costs that affect decisions when acquiring land and issuing a respective building permit, being thus fundamental to the scenario implementation.

1 Introduction

1.1 Aniketos motivation and background

The Future Internet will provide an environment in which a diverse range of services are offered by a diverse range of suppliers, and users are likely to unknowingly invoke underlying services in a dynamic and ad hoc manner. Moving from today’s static services, we will see service consumers that transparently mix and match service components depending on service availability, quality, price and security attributes. Thus, the applications end users see may be composed of multiple services from many different providers, and the end user may have little in the way of guarantee that a particular service or service supplier will actually offer the security claimed.

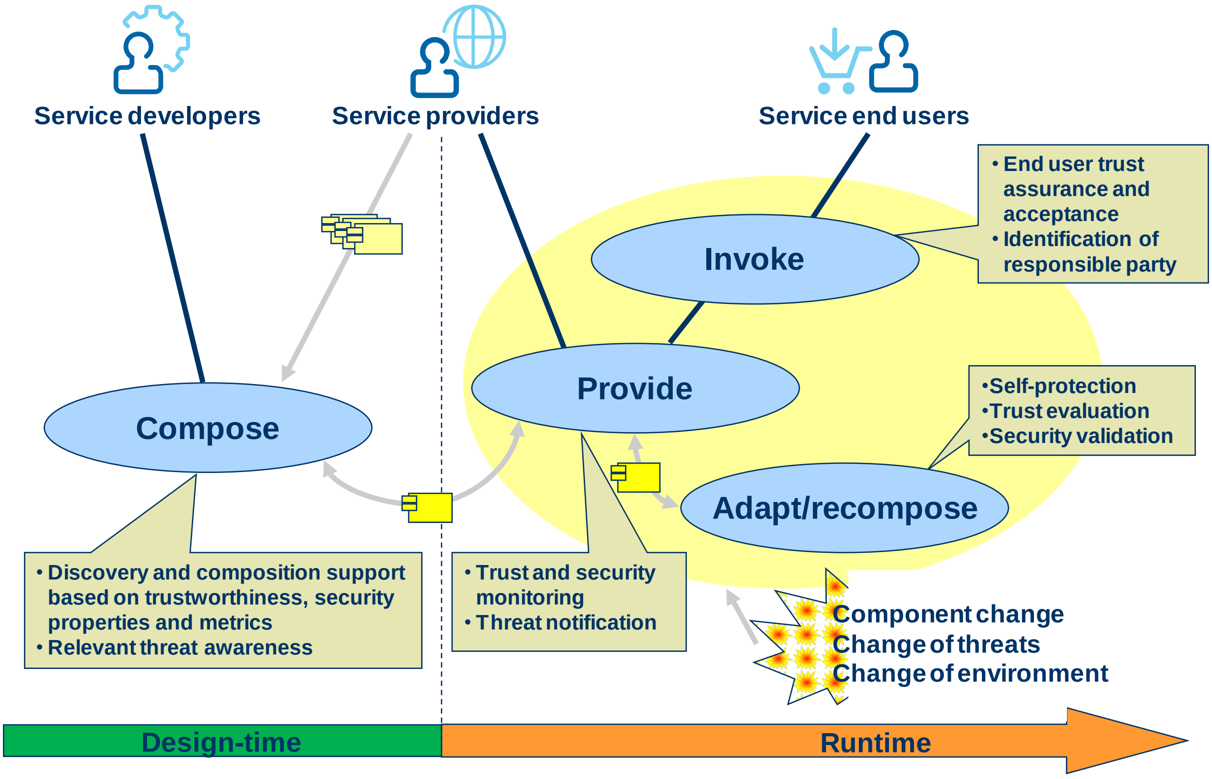


Figure 1: Goal: establish and maintain security and trustworthiness in composite services

Aniketos is about establishing and maintaining trustworthiness and secure behaviour in a constantly changing service environment. The project aligns existing and develop new technology, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service end users.

Aniketos provides methods for analysing, solving, and sharing information on how new threats and vulnerabilities can be mitigated. The project constructs a platform for creating and maintaining secure and trusted composite services. Specifications, best practices, standards and certification work related to security and trust of composite services are promoted for inclusion in European reference architectures. Our approach to achieving trustworthiness and security of adaptive services takes account of socio-technical aspects as well as basic technical issues.

1.2 Summary

This deliverable provides a description of the scope and objectives of the three industrial case studies identified for validating the Aniketos platform.

The case studies are real-life cases in emerging European services so to ensure realism and future relevance.

The industrial case studies will be specified in terms of detailed scenario descriptions, technology domains, platform related requirements and domain specific requirements.

1.3 Relationships with other deliverables

The D6.1 presented in this document relates on the following deliverable:

- D1.2 – First Aniketos architecture and requirements specification: in this deliverable an initial set of functional requirements is elicited. The industrial case studies' aim is to assess these initial requirements and to elicit domain specific requirements, identifying those requirements that can be generalised and that will be fed back to the more general platform requirements of WP1.

1.4 Contributors

The following partners have contributed to this deliverable:

- ATC
- DAEM
- DBL
- ELSAG
- ITALTEL
- SAP
- SINTEF
- THALES
- WIND

1.5 Acronyms and abbreviations

ACC	Area Control Centre	PEN	Pan European Network
AD	Aeronautical Data	PENS	PEN Service
AIS	Aeronautical Information Service	PMU	PENS Management Unit
AMAN	Arrival Manager	PSSG	PEN Service Steering Group
ANSP	Air Navigation Service Provider	PUG	PENS User Group
AOC	Airline Operational Control	RBT	Reference Business Trajectory
AOR	Area of Responsibility	SD	Surveillance Data
APOC	Airport Operation Centre	SM	SWIM SW/MDW
ASM	Air Space Management	SOA	Service Oriented Architecture
ATC	Air Traffic Control	SSO	Single Sign-On
ATCO	Air Traffic Controller	SW	Software
ATF(C)M	Air Traffic Flow (and Capacity) Management	TWR	Tower
ATSU	Air Traffic Service Unit	UAC	Upper Area Control
CAA	Civil Aviation Authority	UAS	Unmanned aircraft system
CD	Capacity and Demand Data	UAV	Unmanned autonomous vehicle

CFMU	Central Flow Management Unit	VFR	Visual Flight Rules
CONOPS	Operational Concept	VLJ	Very Light Jet
ECAC	European Civil Aviation Conference		
EU	European Union		
EUROCAE	European Organization for Civil Aviation Equipment		
FD	Flight Data		
FDP	Flight Data Plan		
FIdM	Federated Identity Management		
FIS	Flight Information Service		
FO	Flight Object		
GA	General Aviation		
ICAO	International Civil Aviation Organisation		
ICD	Interface Control Document		
ICOG	Interoperability CO-operation Group		
IdP	Identity Provider		
IFR	Instrument Flight Rules		
IOP	Interoperability		
IPR	Intellectual Property Right		
JU	Joint Undertaking		
MDW	Middleware		
Navaid	Navigation Aid		
NGN	Next Generation Network		

Table 1: Acronyms and abbreviations

1.6 Change log

No change log entries.

2 Case study A: “Future telecommunication services”

2.1 Introduction

Telecommunication domain is an area of constant change, with tough competition between service providers. It involves threats related to privacy and fraud that concern user acceptance and trust issues for ordinary citizens.

The level of competition in the telecommunication sector is getting intensified as private operators are looking for enhanced telecommunication services to further increase their revenue from mobile and Internet services. Telecommunication operators leverage on Web services paradigm to provide a new set of integrated IT and Telco services**.** Telecommunication services may be grouped in two categories:

- Telco specific services;
- hybrid services.

The main characteristics of the services belonging to the first category are strong real-time requirements and asynchronous interactions. These are typically deployed in network environments strongly controlled by Telco operators. Typical examples of this service category are Voice mail, call forwarding and ring back tone. Web service paradigm is unsuitable for this service category.

Hybrid services integrate different IT resources with Telco functionalities. Web Service paradigm is well suited for this service category that therefore could benefit from the usage of Aniketos platform.

Case Study A focuses on the possible evolutions of the telecom (TLC) operators’ role in the Future Internet landscape. Internet has grown in popularity and importance, and its cheap and easy-to-manage Internet Protocol (IP) is being quickly extended to other networks. In order to face competition with the Web Service Providers, TLC operators are considering an open-platform business model in order to provide services which are exposed and consumed by using Web 2.0 service technologies, i.e. the so-called Telco 2.0 approach. Around this model, it is possible to provide and benefit from useful ancillary services that TLC operators are used to manage, such as integrated billing, accounting and customer-relationship management. Moreover, in a converged environment, the integrated operator is also well positioned to offer other profitable services related to customer information, like presence, location, user profiles, and so on.

It should be noted that Web services used in telecom networks have a number of constraints, mainly related to issues of trust when it comes to collaborating with third parties or other operators, as well as the protection of the access to the network and to customer-identity resources. Identity management is the discipline that can provide solutions to these problems, facilitating a secure, reliable, extendable and profitable Web service ecosystem around TLC networks: it commonly refers to the processes involved with the management and selective disclosure of user-related identity information while preserving and enforcing privacy and security requirements. Federated identity management allows the establishment of trust relationship among different entities (service providers, operators, users).

The aim of this case study is to demonstrate how the Aniketos platform can effectively manage the creation of trusted composite services in a convergent TLC environment.

In the next subsections we will give an overview of the main elements that define the case study domain and that will be involved in the realization of the case study: the NGN network and the Federated Identity Management technology.

2.1.1 Next Generation Networks (NGN)

The ICT sector is driving a new era in technological development: the migration to fully Internet Protocol (IP) enabled networks and services or Next Generation Networks (NGN). NGNs are managed broadband networks that allow integrated data, voice and video services through the deployment of Internet Protocols. IP based networks will ultimately replace traditional circuit switched telecommunications networks (PSTN) and services and traditional fixed line carriers have begun to invest in and deploy IP based networks, usually as overlays of their existing networks which continue to offer traditional services. Due to the efficiencies and flexibility of IP technology, most new networks being established are also IP based. There are numerous views of what constitutes NGNs and different operators that have begun the process of migration or development refer to their networks differently.

The ITU defines a NGN as a packet-based network able to provide services including telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

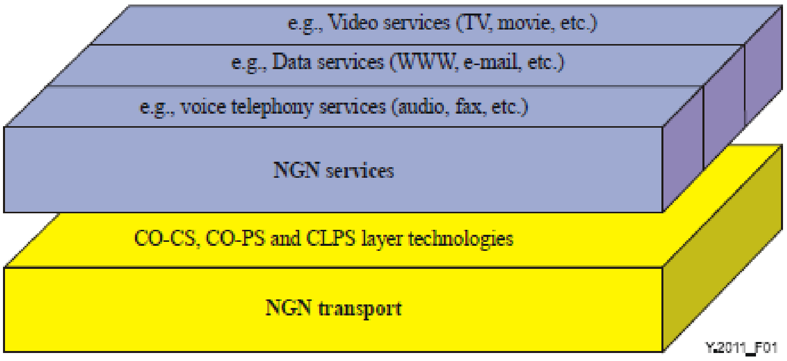

e.g., Video services (TV, movie, etc.)
e.g., Data services (WWW, e-mail, etc.)
e.g., voice telephony services (audio, fax, etc.)
NGN services
CO-CS, CO-PS and CLPS layer technologies
NGN transport
Y.2011_F01

Figure 2: Separation of services from transport in NGN (*from ITU-T rec.* Y.2011)

In an NGN, there is a more defined separation between the transport (connectivity) portion of the network and the services that run on top of that transport. This means that whenever providers want to enable a new service, they can do so by defining it directly at the *service layer* without considering the *transport layer* - i.e. services are independent of transport details. In general, any and all types of network technologies may be deployed in the transport stratum, including connection-oriented circuit-switched (CO-CS), connection-oriented packet-switched (CO-PS) and connectionless packet-switched (CLPS) layer technologies.

Moreover, the above definition divides the NGN transport in two parts, namely the *core* and the *access*. The *core* uses digital technology to connect telephone calls and other network traffic more efficiently than traditional networks. Building a *core* does not directly influence *access* technologies. This facilitates converged technologies to carry multiple services (voice and data) over the *same* (horizontal) infrastructure and equipment, rather than using *separate* (vertical) equipment and/or infrastructure.

2.1.2 Identity Management and Federation

In order to provide a secure access to resources and personalized services, end-users are required to provide their identity. An identity consists of traits, attributes, and preferences. End-users can access a huge number of resources such as merchandise web sites, online banks, tax services, payroll services, email service, so multiple identities are a norm and proliferation of identities creates a major challenge. In this context, the problem of handling the issues related to the overall **Identity Management** arises, namely all policies, processes and technologies that establish user identities and enforce rules about access to digital resources. Identity Management represents a very important issue and Telecommunication companies are strongly supporting the evolution toward Federated Identity Management.

In a campus setting, many information systems such as e-mail, learning management systems, library databases, and grid computing applications require users to authenticate themselves (typically with a username and password). An authorization process then determines which systems an authenticated user is permitted to access. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled.

Federated identity management extends this approach above the enterprise level, creating a trusted authority for digital identities across multiple organizational security domains.

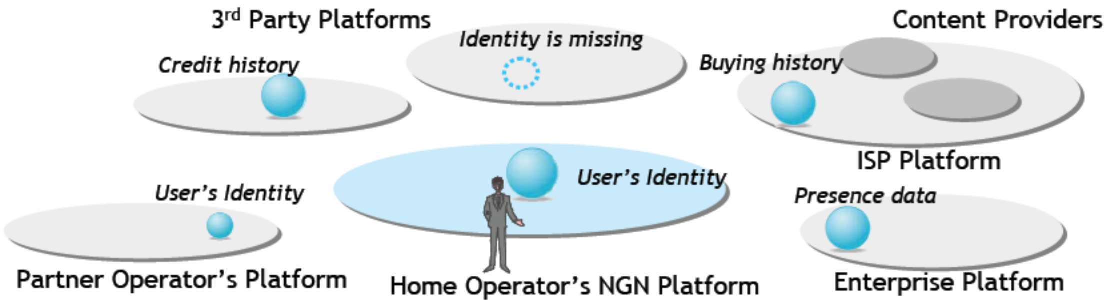


Figure 3: Identity fragmentation (*from ITU-T*)

Federated identity refers to a situation in which one organization (the Identity Provider, or IdP) verifies the identity of a user, and another organization (the Service Provider, or SP) provides services to that user. Examples are an employer (IdP for its employees) and an employee benefits company (SP) with a web-based employee benefits portal. Instead of each organization having to maintain duplicate user identity information, and therefore bear the cost of maintaining it, the employer keeps the user identity information, and the benefits company trusts the employer's authentication. The user is only required to sign on once, not at every website. Therefore federated identity management transfers the responsibility for identity management (and the resulting cost) to identity providers who are better positioned to fulfil that responsibility.

Federated Identity Management goes beyond the technical details of how servers communicate with each other. It is that technology plus business agreements and policies that govern who may access which services, and for what business purposes. These systems enable two organizations to agree on a common identity for the user of a computer system, even though privately they may each have different definitions of that user. It's a way of linking together the user's two separate profiles via a common definition that two trading partners agree to share. Furthermore, the shared definition is obscured (hidden) and only used between one pair of IdP and SP services. If it is exposed, it cannot be used to log in anywhere else.

When the architecture separates the identity information's source from its usage, everyone benefits:

- Users can log in once - with one set of credentials - and access multiple Web sites without revealing their credentials to all of them.
- SPs can delegate many account-management tasks (such as password resets) and receive accurate just-in-time user data.
- IdPs can focus on improving authentication methods and adding attractive features to account-management interfaces.

Federated identity management is a set of technologies and processes that let computer systems dynamically distribute identity information and delegate identity tasks across security domains. Federated identity is the means by which Web applications can offer users cross-domain single sign-on (SSO), which lets them authenticate once and thereafter gain access to protected resources and Web sites elsewhere. However attractive its benefits, federated identity imposes costs as well, entailing new and increased security and privacy risks because it shares valuable information across domains using loosely coupled network protocols. Such risks require mitigation, which can range from preventing message replay to collect user consent for data sharing in both online and offline scenarios.

2.2 Security and trustworthiness problems

The realization of the case study will bring to the creation of a framework which results from the integration of a Federated Identity Management system with the modules of the Aniketos platform and the modules of the environment. In order to simplify the interaction among the several components, we could think the framework as made up of three main systems:

- Aniketos platform, that will offer the core features for the design and development of secure and trustworthy composite services;
- FIdM, the system in charge of managing processes and tasks that involve identities and identity related information;
- Environment, made up of tools that support the execution of the composite services.

The main purpose of the framework we are going to design is to allow an end user to invoke a customized composite service that, in order to be executed, needs a piece of his/her personal identity data. Digital identity of a user and personal identity information are managed by a Federated Identity Management system.

When an end user invokes a composite service, the three systems making up the framework interact by exchanging the user’s personal information needed to carry out their tasks, thus allowing the execution of the service.

From this simplified but emblematic scenario emerges that digital identities and identity related data are the most valuable asset, so in the following we will focus on potential risks and threats to user privacy and possible countermeasures.

The introduction of a federated identity management system enables the dynamic use of distributed identity information, simplifying the user experience in accessing multiple services but it also carries potential risks to privacy.

Federated identity management is basically the means by which web applications can offer users cross-domain single sign-on, which lets them authenticate once and thereafter gain access to protected resources and Web sites elsewhere. In order to offer this capability federated identity management systems share valuable information across domains using loosely coupled network protocols, so it entails privacy risks that require mitigation, which may range from preventing message replay to collecting user consent for data sharing.

Ideally, in order to exchange identity claims in a secure manner, all parties involved should secure their communication channels against replay attacks, man-in-the-middle attacks, session hijacking, and other threats that allow malicious use of user information or web resources. In an HTTP context, channels can be secured considering Secure Sockets Layer/Transport Layer Security (SSL/TLS) with mutual authentication as a security baseline.

The authentication method is another weak link in the web identity chain. Currently, most sites rely on username/password pairs because this method poses the smallest initial burden for users and site administrators. However, it’s notoriously weak and susceptible to phishing attacks.

For service providers, federated identity is less expensive than implementing a high-quality authentication infrastructure because it offloads the authentication task to an IdP. However, IdP-based SSO can magnify the costs of a stolen password because it expands the scope of malicious activity. Most SSO protocols offer ways to mitigate this risk, for example limiting to a minute or less the valid lifetime of the security token that an IdP sends to the service providers.

In FIdM systems another source of privacy risk to be countered is the inappropriate, excessive and without consent data disclosure. To mitigate this risk FIdM systems should use the principle of minimal disclosure providing personal identity data only on a need-to-know basis, and should allow information to be distributed with each service provider receiving exactly the information needed for its task.

In order to minimize the threats to the privacy the access to the identity data must be authorized. A FIdM offers the end user a way to control the identity data exchanged with service providers. When the user subscribes to a FIdM, the IdP stores his/her identity related data as a user profile that the user can decide to not share among all the federated service providers. The end user could decide to be informed when the service provider needs a piece of her identity information so that, every time a service provider asks the IdP for information stored in the profile, the IdP asks the user if she wants to share that information.

This situation could lead to another privacy risk. In fact the user could get annoyed by the confirmation requests and could decide to share the whole profile. In this way, all the service providers belonging to the federation share all the personal identity information related to an end user. As a countermeasure, the Aniketos platform should provide guidelines and suggestions on how to model and develop services that will not annoy end users with constant confirmation requests related to trust and security.

Privacy issues arise when considering customized web services that need personal information in order to offer their functionality. As an example, we can consider services which use information about the user’s position. This kind of information constitutes personal information and their improper use violates user's privacy. So, strict ethics and security measures are strongly recommended for services that use positioning information, and the user must give an informed, explicit consent to authorize the service provider to use positioning data from the end user's mobile phone.

Malicious service providers pose a threat to privacy. They could demand for identity information and identity related information, such as credit card number, and sell them to people wanting to commit economic frauds. This threat could be relatively limited choosing services that request the minimum amount of information.

Service composition raises privacy concerns too. Privacy could be violated composing on-the-fly atomic services that, in isolation, wouldn’t pose a threat to privacy. Aniketos platform functionalities should allow modelling the composite services and detecting the threats to privacy.

2.3 Analysis of existing solutions

2.3.1 Service platforms for NGNs

Service platforms in Future Internet shall be targeted at overcoming the current fragmentation in Web and Telecom services, often developed and deployed as ad-hoc silos, by sharing and integrating a number of disparate network resources and backend management systems.

At present, many of the capabilities required for building new services are already implemented within the network, but are scattered across various data repositories and different service execution environments. For example, solutions may already be in place for location and presence information, group list management, calling capabilities, file streaming, content management, real-time payment and others, but these capabilities are often only used and accessible from a so-called stove-pipe service solution. The challenge is to leverage distributed information and expose these assets from different service execution environments, in a uniform way through open interfaces. This will enable the creation and mash-up of new and compelling services quickly and cost-efficiently, leveraging common IT technologies, methodologies and best practices.

Service platforms evolution in the Future Internet has a twofold perspective, from telecommunication infrastructure side and from web site:

- Regarding the telecom network, an important factor enabling a successful deployment of NGN services will be the transition towards the all-IP network infrastructure. The IP Multimedia System (IMS) is considered today as the unifying architectural framework for the provision of seamless IP based services on top of converging fixed and mobile networks. The access agnostic framework of IMS is key to enable the rapid deployment of services, since the IMS overlay architecture is widely abstracted from its interfaces and ensures that the access will be network, technology and vendor independent. Such an architecture model allows and leads to the so called *network* *virtualization*, for which here we refer to the adoption of an “encapsulation” approach to hide the complexity of the telecom core services and to provide an easy to use interface for applications. The service layer of IMS, on top of its core control functions, provides the ground on which service enablers are defined and used for the implementation of composite services.

- At the same time, the evolution of the Internet should be considered, where the new era of Web 2.0 services has emerged, exhibiting the principle of viewing users as active contributors. This will leverage the collective intelligence of large number of users, adopting a light weight model enabled by loosely coupled systems that are simple to use and creating valuable data pools that are difficult to recreate. Popular services like social networking, blogging, mash-ups, social tagging and community-based music services can take advantage of the well-defined IMS framework for further advancement. Telecom network assets could be opened to evolve Internet services while adopting the Web 2.0 principles to enrich services for IMS users. As a consequence, the mix of these technologies could be considered as an enabling platform for boosting innovation and, at the same time, for reducing the cost and deployment time of NGN services.

The disrupting use of Web service technologies can now be seen as the candidate for opening up the networks and exposing capabilities to third party service providers and enterprises. Service exposure capability could be extended, beyond traditional voice and messaging services, also to the abstraction of user authentication and authorization, identity management, policy enforcement, service level agreement, accounting, provisioning and management. The reuse of an extensible set of existing service components to create rapidly new market driven applications has been a key aspect of telecommunications platforms for many years and gains a new momentum with the definition of dedicated application enablers for NGNs.

Service Oriented Architecture (SOA) technology provides the integration framework, suitable for rapid discovery, creation, composition and deployment of services, integrating disparate telecommunication domains in a coherent environment, thus helping to shorten time to market.

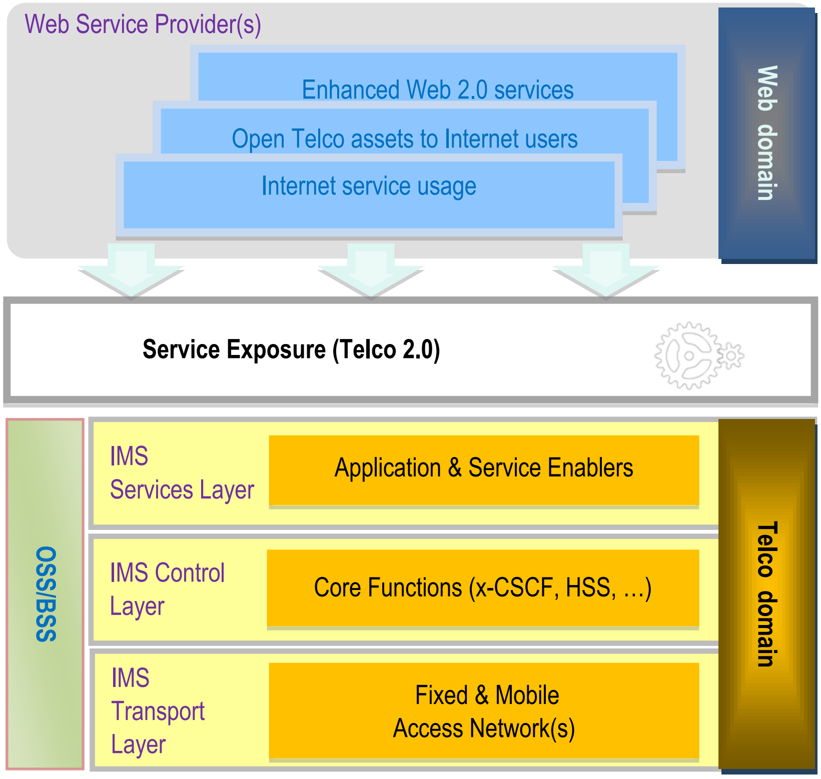

Web Service Provider(s)
Enhanced Web 2.0 services
Open Telco assets to Internet users
Internet service usage
Web domain
Service Exposure (Telco 2.0)
OSS/BSS
IMS Services Layer
Application & Service Enablers
IMS Control Layer
Core Functions (x-CSCF, HSS, ...)
IMS Transport Layer
Fixed & Mobile Access Network(s)
Telco domain

Figure 4: Structure for NGN/IMS/Web2.0 service delivery platform

Standardization initiatives like those lead by Parlay(X) and OMA have specified several standard Web Service interfaces to the most common Telco functionalities, opening them to the IT community. However, adapting telecommunication functionalities to standard interfaces (APIs) is not trivial, because most of the specifications don't provide support for asynchronous interaction. A solution to this problem is adopt an event-based service platform compliant to the Service Logic Execution Environment (SLEE) standard, that overcomes the limitations of SOA-based application servers designed only for enterprise services. The methods and techniques that will be used for network abstraction in Aniketos require further investigation.

2.3.2 Identity Management solutions

In a general IdM architectural model an Entity (User) seeks for a service from a Service Provider (SP) - or Relaying Party (RP) - and provides a claimed identity to that party. The RP needs to have these credentials authenticated before providing the service, so it queries the Entity for the name of the Identity Provider (IdP) for the claimed identity. The RP then queries the IdP for validation of identity that may return some attributes of that identity.

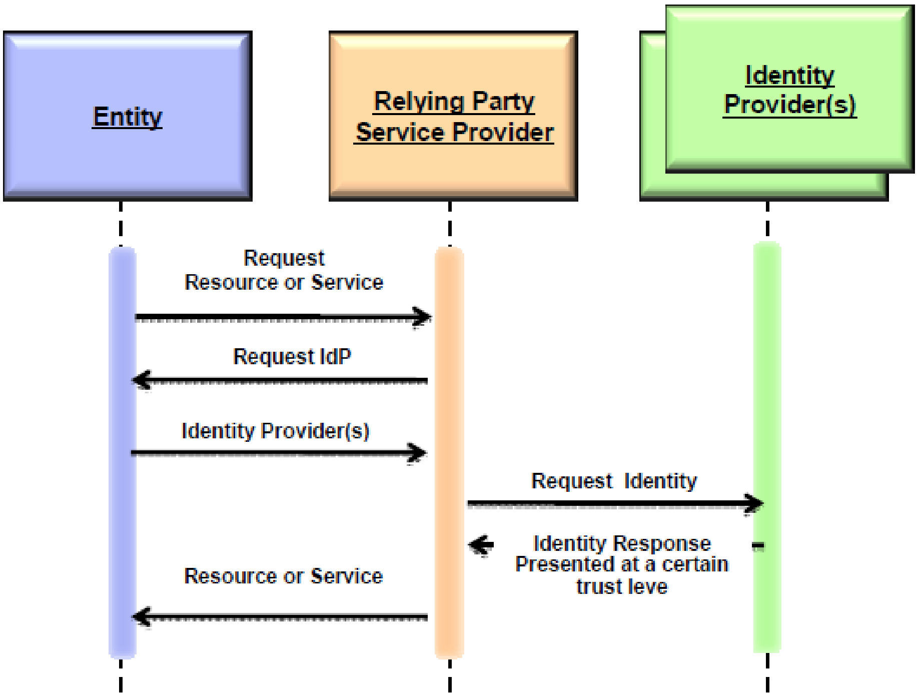


Figure 5: Identity Management architectural model

There is no restriction on who provides IdP services. An IdP is an entity that creates, maintains and manages trusted identity information of other entities (e.g., users/subscribers, organizations, and devices) and offers identity-based services based on trust, business and other types of relationships.

In SSO, data about identification, authentication, and sometimes attributes flows from the IdP to the SP. However, SSO has several variants, each of which dictates a different flow and data exchange:

- *IdP-initiated SSO* or portal-based applications, in which there is a pre-determined number of SPs that can be seamlessly accessed by users with a single authentication. This case, also known as pre-determined federation, can be easily achieved by an agreement stipulated among parties which is statically pre-configured in IdP location.
- *SP-initiated SSO*, which requires an IdP discovery mechanism: the user must have to input his/her IdP thus having a *simplified* (instead of *single*) *sign-on* experience. In this case, applications can also be delivered by SPs outside the domain of trust. These can be accessed by the user, but the authentication process requires that each SP sends to the IdP an explicit authentication request. An improvement could be to provide mechanism(s) in order to perform this task automatically.

In a multiple service provider environment, it is possible for a Next Generation Network (NGN) provider to be an identity provider. It is also possible for an NGN provider to offer IdP services (e.g., identity-based services) to other providers. In addition, it is possible to use third party IdP services.

The majority of user authentication schemes today still use user-id and password. The burden to users of managing large numbers of user-ids and passwords has led to proposals for Federated Identity systems, where a single set of credentials can be used to authenticate with several organizations, which have agreed to work together as a federation. Identity Management requirements in the digital world are well researched, and many solutions are available in today’s marketplace.

2.4 Users definition

Users can be roughly grouped into two categories: end users or consumers and developers.

End users will be mainly those who will access and make use the various services available, with dynamic composition features, that are offered on-line. These services will be accessed typically (but not only) using mobile devices or terminals like for example smartphones, PDAs, Tablets, netbooks or similar equipment with connection capabilities either mobile or fixed. The services are accessed and consumed by means of a web-interface typically using a web-browser.

Developers will be mainly those who will use the Aniketos framework (tools, modules, development-environment, etc.) to produce a series of services that can be dynamically composed/adapted while maintaining specific trust and security requirements. These services will be then later offered to the end users typically through web-portals of the various service providers or telecom operators. The developers can be either service providers or telecom operators or associated third parties who are in charge of producing some kind of service offered on-line. A more specific definition of what developers do is given below.

The developer designs and implements pieces of the solution and tends to have specialized skills that focus on a development platform, programming language, and/or business area. The following types of developers are typically involved in building service-oriented solutions.

2.4.1 Service Provider (SP) or Relying Party (RP)

Role

RP/SP

- authenticate the identity before providing the resource or service;
- query the user, also called Entity in the context of Identity Management for the name of the Identity Provider(s) for the claimed Identity;
- query Identity Provider(s) for validation of the claimed Identity (and for the attributes of that Identity).

Services offered:

In this case the composite application is related to the e-commerce landscape. In particular, the selected applications will be developed by using the following services:

- WebShop, a service available for electronic commerce;
- WebTravel, a service that will be used for hotel and ticket reservation.

Services consumed:

The WebShop is a composite service made up of:

- VoIP, an help-desk service;
- StoreLocator, a service used for locating shops.

The WebTravel is a composite service made up of:

  - a web service to book the hotel;
  - a web service to buy the tickets for the trip.

All the above services interact with the Identity Provider service.

Expectations: Services can benefit from Aniketos in increasing their popularity by fulfilling user expectations in security and privacy.

2.4.2 TLC Operator

Role

The TLC operator uses Aniketos to design and offer secure and trustworthy composite services using the features and technologies of the platform.

Services offered:

The TLC operator provides communication services (such as VoIP-based click-to-call capability) and customer information services like presence and location (when allowed by the users).

Service consumed:

All the services aggregated into the TLC operator’s portal.

Expectations: By using Aniketos, the TLC operator is expecting to increase business opportunities by offering to its customers a set of secure services complemented by an identity federation system.

2.4.3 Entity or user

Role

The entity or the user is a requestor who has a digital identity and identifies itself to the Relying Party or Service Provider to request a resource or service from the Relying Party.

Services offered:

None

Services consumed:

All the services available from the portal of the TLC operator.

Expectations: Since every atomic service usually requires the user to login with different credentials, users can positively evaluate the benefits offered by IdP services, i.e. the capability to have access to all the applications in the domain of trust of the operator with Single-Sign-On (SSO).

2.4.4 Identity Provider (IdP)

Role

A suitable IdP will be included in the framework for Identity Management and federation. The IdP authenticates the claimed Identity, and may return attributes of the Identity to the RP/SP. It uses trust mechanisms and security policy to process Identity requests from the RP.

Services offered:

Identity management:

- Authentication
- Authorization
- Secure exchange of data.

Federation

Services consumed:

None

Expectations: TLC operators are well positioned to play the role of both the identity provider and the discovery services entities, as they know all about their customers and have already established a solid relationship with them. In addition, they have already signed business agreements with 3rd parties situated either within their private networks or on the Internet, thus defining a trusted domain.

2.4.5 Developers

Role

We can identify three different roles for a developer: application developer, component developer and integration developer.

The application developer understands the business area for a solution and implements the application code that performs the business-related function. She/he works from a specification of the service interface provided by either the software architect or another developer.

The component developer codes self-contained chunks of code called *components*. These components are designed to be reused in multiple applications.

The integration developer is responsible for building services by configuring components and linking them together. These components could have been written by a Component Developer or provided as part of an ESB product. Integration developers typically have a good understanding of integration techniques and patterns but limited programming skills. If an integration scenario requires some complex programming logic, an Integration Developer works with a Component Developer to create a new component for the integration.

Service offered:

Atomic or composite services to be advertised and to be offered through the Aniketos marketplace.

Service consumed:

Services components and composite services exposed in the Marketplace.

Expectations: The developer can exploit Aniketos Marketplace to discover services by specifying security and trust properties and can create secure and trustworthy services to be offered to other developers through the exposure in the Aniketos Marketplace.

2.5 User stories description

In order to increase its business opportunities, a TLC operator decides to exploit Aniketos design time and runtime support for secure and trustworthy service composition.

In particular the Telco operator wants to exploit Aniketos platform to:

- discover service components that conform to its security requirements in order to build composite services or web applications featuring the desired level of security and trustworthiness (User Story A1)
- expose its network resources as services in the Aniketos Marketplace (User Story A2)

2.5.1 User story A1

The exploitation of the Aniketos features will allow the TLC operator's potential partners and end users to trust the security properties declared for its services, since the Aniketos platform provides the means to monitor service components exposed in the Marketplace.

In the particular case of the User Story A1, the TLC operator is planning to develop a web portal so to offer a set of applications to its customers. The application developer, who is responsible for developing the portal using Aniketos platform, will use the Aniketos Marketplace to discover service components which offer the functions he needs to build the application logic. The usage of the Aniketos platform enables the developer to discover service components also based on security and trustworthiness properties. The discovery features provide him with a list of service components among which he has to choose the components that best fit the security requirements specified by the TLC operator. In this case he chooses the components having a level of trustworthiness above a predefined threshold (freely chosen by TLC Operator).

The realization of the user story A1 will result in the development of a framework based on web services exposed in the Marketplace and supported by Federated Identity Management technologies. As a result, in this case study technologies offered by Aniketos platform will be tied to the usage of an

Identity Management system. The practical advantage for the users is that only a single authentication is needed for having access to the whole set of applications in the trusted portal domain.

User story A1 is described from the point of view of an end user that utilizes the applications and services accessible through the TLC operator's web portal. Basically the web portal collects and composes services offered by third party Services Providers joined with the TLC Operator in a federation for the identity management.

In the following table the description of the main user story is provided.

User story A1 – Bob accesses services offered through a TLC operator's web portal and provided by different service providers joined with the TLC operator in an identity federation	
Description	Bob, a new user, subscribes to the portal offered by the TLC Operator, and at the end of the registration process he gets a username and a password to login. Bob wants to browse through the portal by using his smart-phone using a Wi-Fi connection. The smart-phone has GPS capabilities and it is provided with a presence-enabled VoIP client. Bob provides his credentials, namely username and password, to login to the portal. From now on, he is authenticated to *all* the applications belonging to the federation. Bob browses the portal and accesses WebShop application to purchase an item. Since he wants to get more information about a specific product, he uses the link on the web page in order to start a click-to-call VoIP communication with a selling assistant. Once Bob has got information he needed, he decides to purchase the item he was interested to. He chooses the "Store pick up" as shipping option, so the StoreLocator service is provided in order to let the user choose the store where to pick up the item in person. Bob is informed that the StoreLocator service, in its basic configuration, will let him to select manually the preferred store from a list and will show the position of the store on a map. Otherwise he can give his authorization to use his position information: in this case the StoreLocator service will use this information in order to help him to find the closest store. Thus the StoreLocator service composition is driven by Bob decision to give or not his consent to use his position. In particular, if Bob decides to not give his consent, the StoreLocator service is a simple component that shows on a map the store selected by Bob. If Bob decides to let the service use his position information, a recomposition takes place. In this case the StoreLocator service is made up of three components: • a service that, when invoked, returns location information of the user; • a service that receives location information as input and gives as result the list of the closest stores; • a service that receives the list of address of the closest stores and show them on a map. Bob selects the store where to pick up the item from the list returned by the StoreLocator service. Bob is asked to confirm the mail address (retrieved through the IdP) to be

	informed when he can go to pick up the item. Then, via a direct link offered in the portal, Bob connects seamlessly to the WebTravel application in order to book a hotel and the tickets for his next business trip. WebTravel is an Internet based application built using a composite service made up of two service components: • a web service to book the hotel; • a web service to buy the tickets for the trip; These two services are included in the composition at design-time. In order to complete the hotel reservation, an electronic form must be filled with personal data. The system detects, through the presence information, that Bob is currently using a smartphone so, in order to help him to fill the form Bob is asked to give this authorization for the automatic compilation of the reservation form. Bob accepts and allows the retrieval of this information from the IdP in a secure manner.
Involved roles	TLC operator, service providers, IdP, end users
Outcome	The end user can seamlessly access web applications provided by a portal developed by the telecom operator. The telecom operator develops his applications using functionalities provided by Aniketos platform.

Table 2: Case study A - User story A1

2.5.2 User story A2

In a time of deregulation and fierce competition, the revenues of the Telco operators are diminishing every day. The role of carriers in the value chain from devices to applications has shrunk, due to the strong alliances between device vendors and Over-The-Top (OTT) providers that have tended to limit the carriers' role of dumb pipe providers. While device vendors and OTT providers increase their revenues, carriers all over the world are trying to find ways to profit from this traffic and compensate them for the increasingly heavy traffic on their networks. A Google/Verizon joint policy proposal attempts to stimulate regulatory changes and give wireless operators the possibility to differentiate traffic in their networks and to promote investment in new platforms for innovative services.

The success of broadband operators might well depend upon harnessing their assets and evolving their business model according to a new scenario which depends upon developing a partnership ecosystem. The operator's main assets include the ability to manage traffic at different network layers (access network, core network and interconnection domain); access to subscriber data regarding devices, preference profile and usage; and a service platform to provide new services leveraging on network capabilities shared with partners. These assets give operators the means to turn a dumb pipe into an intelligent one - if given some flexibility in the network neutrality principles.

The evolution of Internet applications also requires strong identity management for privacy and security reasons. To be an Identity Provider, as suggested in **2.4.4**, is a natural role for Telco operators as they already possess and manage large numbers of customer identification and authentication data in regards to their own systems and services. In fact, Telco operators:

- are already service providers for their own value added services,
- in many cases also act as identity issuers, either for their own services or increasingly to 3rd parties,
- hold a large amount of information on their customers, which enables them to act as an attribute provider too.

By becoming an IdP, a Telco operator will be able to offer better services to its customers in terms of quality, user-friendliness, cost and variety, thus obtaining new source of revenues and improvement of customer loyalty. On the other hand, the most important advantages for telecom subscribers will be:

- to have access to a larger, more diversified and more geographically distributed services,
- services can be personalized and adapted to the context of the user,
- the burden of having to manage multiple accounts and password will be considerably mitigated.

User story A2 will be based on identity management, just giving an example of how a service provider could expose its services through the Aniketos platform. The following description is from the point of view of a Telco operator that plays the role of a service provider that is willing to build services by using the technologies and the functionalities offered by the Aniketos platform.

User story A2	
Description	WinTel is an important telecom operator that wants to unlock the value of its subscriber data. WinTel has customer information related to network parameters, devices, fixed and mobile lines, email boxes, presence and location and, with restrictions according to privacy laws, the customer's usage profile. By unifying subscribers' data, WinTel operator can expose and broker data to third parties cooperating in the delivering of new services and, finally, play the role of an identity provider trusting authentication and critical transactions across several Internet applications. WinTel wants to advertise a trusted identity provider service through the Aniketos Marketplace to make it available to service developers who want to compose trustworthy services. In particular WinTel will design the service to be exposed in order to provide IdP functionalities for the management of subscribers' credentials and the authentication process for different services. Alice is a service developer who has been assigned by WinTel the task to develop the IdP service and make it available on Aniketos marketplace. Alice accesses and browses Aniketos website to get an overview of the main features of the Aniketos platform. In particular Alice gets that in order to know how to get started and develop new Aniketos compliant services exploiting the Aniketos platform functionalities she has to use the Training material and Community support modules. She wants to specify trust and security properties for the IdP service so she searches for tutorials and guidelines in order to get informed of how to specify these properties in Aniketos framework. Finally, Alice creates the IdP service and submits the service specification to the Aniketos marketplace service registry.
Involved roles	TLC operator, service developers, service providers
Outcome	A Telco operator advertises its Telco services through Aniketos marketplace

Table 3: Case study A - User story A2

2.6 Domain constraints

Domain constraints for this case study are mainly related to the decision to use a Federated Management system to handle user identities and establish trust relationships among service providers.

Several Federated Identity approaches require one organization, namely the Identity Provider (IdP), to be in a privileged position in control of the issuance and/or validation of credentials. This approach limits the application of federated identity, as naturally most businesses do not wish to pass control of a major asset, i.e. their customers, to another entity. It may also imply an asymmetric relationship, where users show their credentials to the identity provider, without necessarily being able to easily mutually verify its credentials. It is frequently difficult to mix different credential verification services within an organization; the implementation assumes the same technology will be used throughout.

Additionally, several Federated Identity approaches combine user credentials (proof of identity) with user attributes (such as personal data). This leads to potential privacy issues, which may also cause legal problems, especially if the credentials and attributes are passed across national borders. Complex proposals have been made to allow the user to control which attributes may be passed between organisations.

Despite the benefits of federated identity, the up-front costs to modify existing applications and systems can be an obstacle for some institutions. Federation membership might require different or more stringent identity protocols than an institution currently observes, and an institution might participate in multiple federations, each with unique requirements. Participating in a federation requires developing thorough institutional policies concerning access rights and compliance with the complex landscape of regulations. Although such policies and the work involved in writing them are beneficial, some institutions might not be ready to undertake such an effort. The risks associated with unauthorized access to certain services are sufficiently high that provider organizations sometimes demand additional assurance from federation members. In these cases, a federation member might follow guidelines that set a higher bar for ensuring that credentialed.

There are some common business and technical challenges that must be solved. Technical challenges must be managed within the constraints of existing business and legal agreements between organizations that define thresholds for acceptable use, risk and indemnification.

2.7 Domain specific requirements

In this section, requirements related to the case study are collected.

2.7.1 Security requirements

Requirement ID – Type:	6A.1 - F
Requirement Name:	Circle of trust
Description:	Service Providers should be enabled to create Circle of Trust (CoT) domains among SPs and an IdP in a pre-defined manner.
Rationale:	Circle of trust will allow an end user to access services provided by different service providers authenticating once.

Requirement ID – Type:	6A.2 - F
Requirement Name:	Trust relationships
Description:	The Aniketos platform should support the use of a mechanism that allows service providers to establish trust relationships between them.
Rationale:	The establishment of trust relationships is the key concept enabling SSO technology.

Requirement ID – Type:	6A.3 - F
Requirement Name:	Secure critical data exchange
Description:	Service end users should be assured that their critical data will be securely exchanged.
Rationale:	Identity and identity related data are assets that the service end user wants not to be disclosed to unauthorized entities.

Requirement ID – Type:	6A.4 - F
Requirement Name:	Consent to usage of identity related data
Description:	The end user should be informed when identity related data, such as location information, are required by a service provider to offer personalized services
Rationale:	Identity related data can be used only if end user gives his consent

Requirement ID – Type:	6A.5 - F
Requirement Name:	Specify privacy requirements
Description:	The end user should be allowed to specify the identity related data that he wants to be shared by the service providers belonging to the Circle of Trust
Rationale:	The end user is the owner of his identity data and he should be enabled to choose which personal data can be used by federated service providers

Requirement ID – Type:	6A.6 - F
Requirement Name:	Request least set of information
Description:	A composite service should be allowed to request the minimum set of identity information that is necessary to offer the services
Rationale:	The service consumer doesn’t want to give out unnecessary personal information

2.7.2 Technological requirements

Requirement ID – Type:	6A.7 - F
Requirement Name:	Service descriptions in the marketplace
Description:	The Aniketos marketplace should use a service description language that provides information for allowing a security analysis of the offered services and compositions thereof.
Rationale:	Aniketos deals with secure composition, so services in the marketplace must be analysed to provide information about their security aspects.

Requirement ID – Type:	6A.8 - Q
Requirement Name:	Support service developers
Description:	The Aniketos design-time support modules need to come along with sufficient documentation, training, and support for the service developers.
Rationale:	Service developers should be provided information in forms of guidelines and tutorials in order to start using Aniketos platform.

Requirement ID – Type:	6A.9 - F
Requirement Name:	Federated Identity in Next Generation Networks (NGN): telecommunication services
Description:	Aniketos platform should support the use of Federated Identity Management.
Rationale:	In real-life scenarios a user accesses several web applications with multiple identities, so a mechanism to allow the user to authenticate once is required.

Requirement ID – Type:	6A.10 - F
Requirement Name:	Federated Identity in Next Generation Networks (NGN): discovery of IdP services
Description:	Aniketos platform should support the discovery of IdP services.
Rationale:	Since IdP services handle identity data service providers rely on them in order to establish trust relationship.

Requirement ID – Type:	6A.11 - F
Requirement Name:	Leveraging the NGN operators' role in IdP
Description:	Aniketos platform should be able to manage IdP functionalities to/from service providers.
Rationale:	Services that need identity data to perform their task should be enabled to interact with IdPs.

Requirement ID – Type:	6A.12 - F
Requirement Name:	Trustworthiness ranking
Description:	The Aniketos platform should be able to rank services based on their trustworthiness properties.
Rationale:	Services Ranking functionality could be used to ease the service selection based on trustworthiness properties

Requirement ID – Type:	6A.13– F
Requirement Name:	Publish trust properties
Description:	The Aniketos platform should provide a mechanism that allows services to provide information about their trust properties.
Rationale:	Trust properties of a service must be specified in order to let the potential consumer decide if the trust properties fit its trust related requirements.

Requirement ID – Type:	6A.14 – Q
Requirement Name:	Developer center
Description:	The Aniketos platform should have a developer center containing information about requirements and methods of creating Aniketos compliant services.
Rationale:	The developer center should make it easy for developers to build services to be advertised through Aniketos platform.

Requirement ID – Type:	6A.15 - Q
Requirement Name:	Aniketos supportive services
Description:	The Aniketos platform should provide additional, more detailed, and easy-to-find information about its supportive services for design-time and run-time to the service developer
Rationale:	Service developer should be supported to easily start developing services using Aniketos platform.

2.7.3 Run-time requirements

Requirement ID – Type:	6A.16 - Q
Requirement Name:	Composition driven by end user choosing
Description:	The Aniketos platform should allow the user to drive the selection of components for a composite service
Rationale:	The components involved in the service composition could change according to the preferences expressed by the end user at run-time

Requirement ID – Type:	6A.17 - Q
Requirement Name:	Sensitive data handover composition
Description:	Sensitive data should not be handed off to third parties when a service recomposition takes place without user confirmation.
Rationale:	Service end users must authorize that 3rd parties can handle his identity related data

Requirement ID – Type:	6A.18 - Q
Requirement Name:	Notify composite service developer
Description:	The Aniketos platform should alert service developer if their service trustworthiness of the components they use to create composite services falls below a threshold
Rationale:	The composite service developers should be notified so that he can change the components involved in the composition

2.8 Storyboard

The storyboard lists the exact sequence of actions carried out by the users involved in the case study. It represents what will be shown with the realization of the case study. In particular, the storyboard analyses all the activities performed and highlights the interaction of the end users with the system.

The end user scenario is related to the e-commerce landscape, where different accessible services are available. The main services involved are:

a. WebShop for general electronic commerce access;

b. StoreLocator for making users choose the store where to pick up items selected;

c. WebTravel for hotel and flight ticket reservation.

The end user (Bob) is a typical commuter who owns a mobile device (PDA/Smartphone) which is equipped with Wi-Fi interface, a GPS receiver and a presence enabled VoIP client.

The sequence of actions illustrated below shows the sequence of steps an end user will run through by interacting with web services when accessing the web portal of a TLC Operator.

1. **Bob subscribes to the Portal application**

   Bob subscribes to the Portal, by accessing it via any browser interface over the Internet. During the subscription process Bob is asked to specify a brand new user-name and a password. Moreover, he has to fill a form with personal information.

   As a result of the subscription to the Portal, Bob is a registered user and from now on he is allowed to access/use any service offered on the Portal without any additional identification request. That means that he is in SSO (Single-Sign-On) and the services used are part of a Federation of Services.

2. **Bob logs into the Portal application**

   By using his own Wi-Fi enabled mobile equipment, Bob logs into the Portal, accessing it via a browser interface over the Internet. During the login Bob is asked to specify his user-name and password.

Actors and interactions with the Aniketos pilot described in steps 1-2 are represented in the use case diagram in Figure 6.

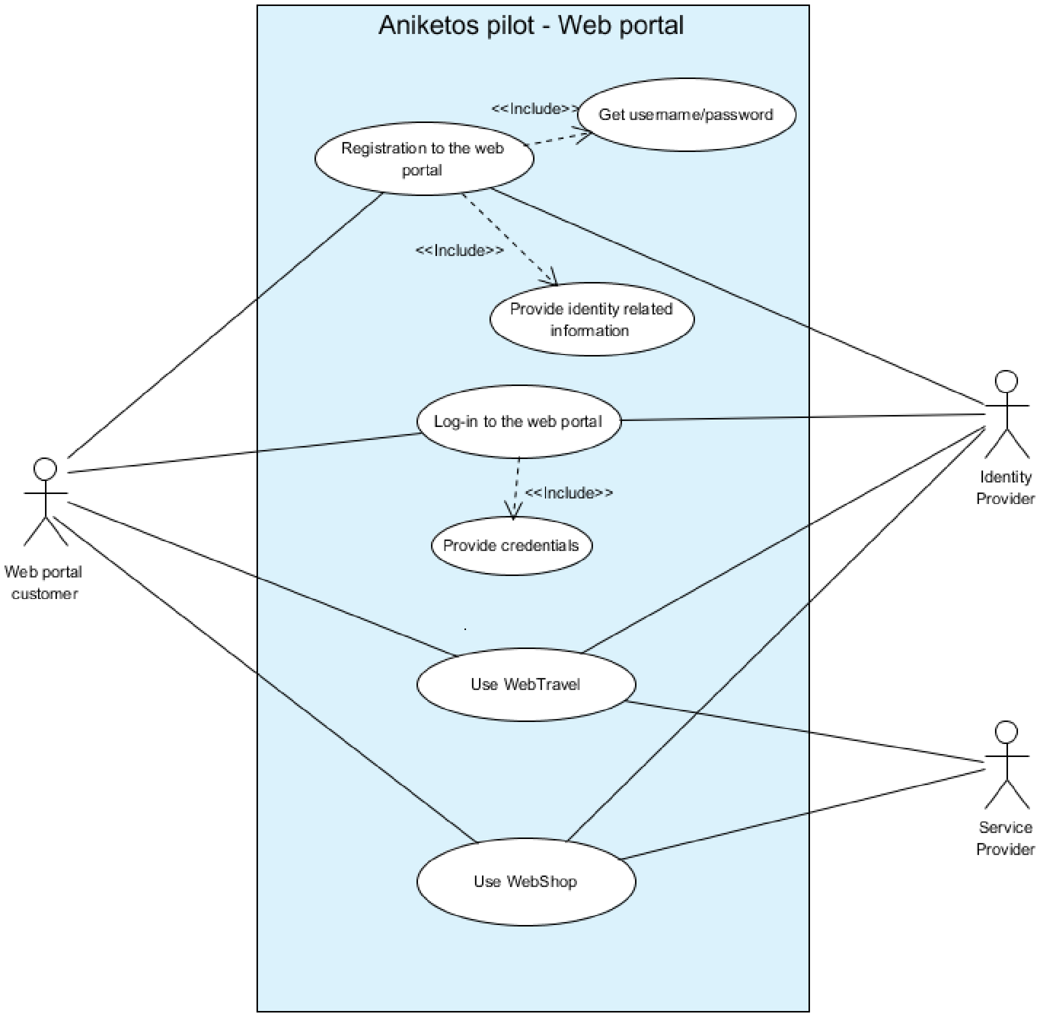


Figure 6: Aniketos pilot – Web portal: use case diagram

3. **Bob accesses WebShop application**

   Bob accesses the WebShop application in order to purchase an electronic item he wishes.

4. **Bob accesses the VoIP service, inside WebShop application**

Browsing through the various electronic articles offered at the WebShop he selects one, but he wishes to get further and more complete information that are not available directly from the WebShop page. For getting additional information he then requests the help of a (human) assistant by starting a click-to-call VoIP communication. Bob can then speak directly with a WebShop clerk in real-time and ask for more detailed information about the product he is interested in and that he wishes to purchase.

5. **Bob select "Store pick up" option and the StoreLocator service is offered**

   Once Bob has got the information he needed, he decides to purchase the item he was interested in. When checking-out from the WebShop he decides to collect the purchased item in person and then selects "Store pick-up" among the various shipping options offered. In this case a special StoreLocator service is offered to facilitate the pick-up by letting the customer choose the most convenient shop for him.

6. **StoreLocator service recomposition, after Bob's choice**

   The StoreLocator service gives users two options, namely: 1) a manual selection of the pick-up stores that can be selected from an offered list; or 2) letting StoreLocator service propose a list of closest stores. The second option can be successfully done only if the user gives his consent to StoreLocator to have access to his current geographical position.

   Bob selects option 2) for automatic store localization. By doing so a service recomposition is started, to collect Bob's current position information and to generate maps and addresses of the stores which are closer to Bob, where he will be able to pick-up the purchased item.

   As a result a map (or a list of addresses if the interface has no graphical capabilities) of the closest pick-up store is generated/displayed on the screen of his mobile phone.

7. **Bob is asked to confirm his mail address**

   Bob is finally asked to confirm his mail address (that was retrieved through the IdP) in order to receive a message (he will see on his mobile phone) to inform him when he can pick-up the purchased item.

Actors and their interactions with the WebShop application described in steps 3-7 are represented in the use case diagram in Figure 7.

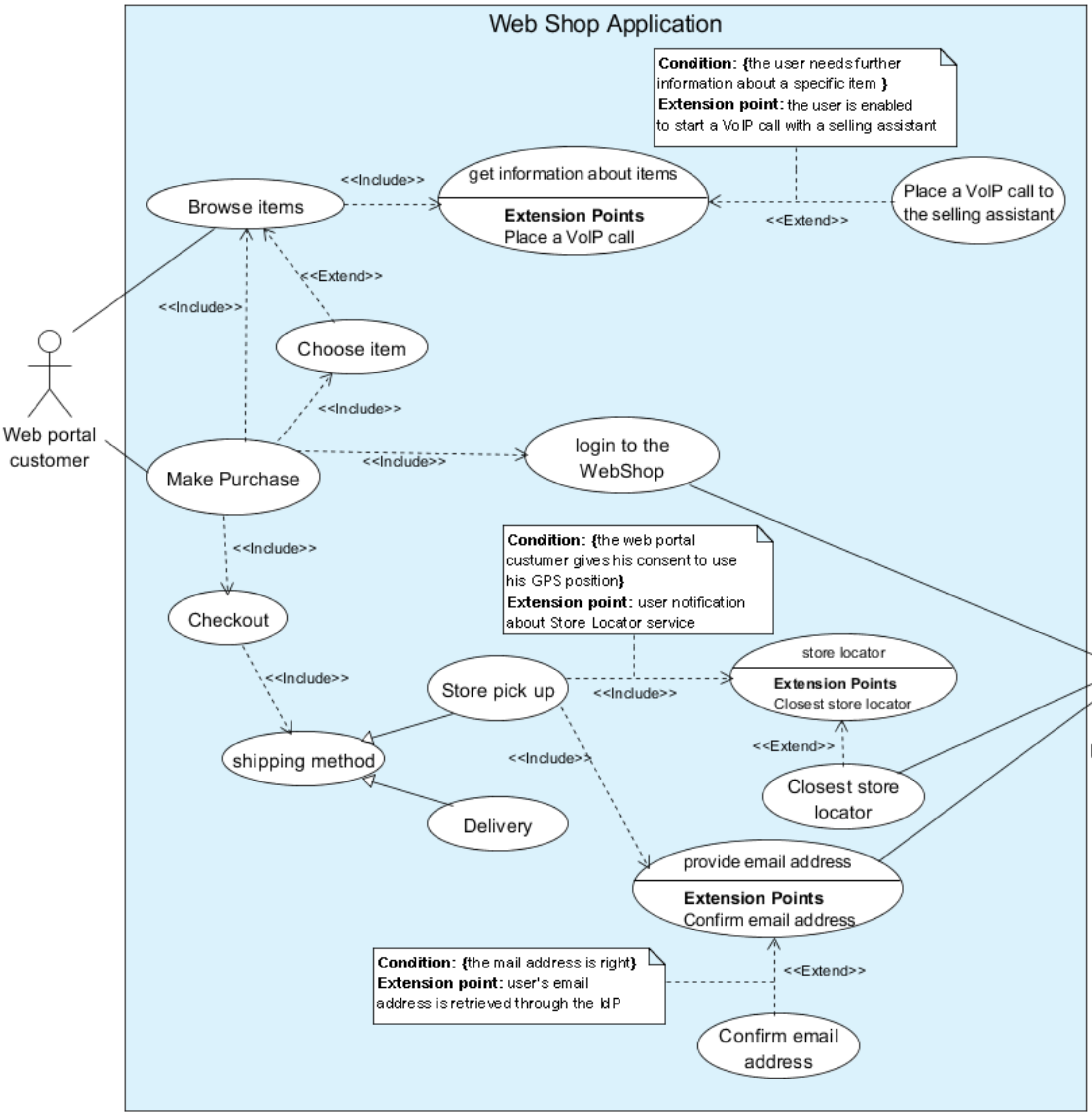


Figure 7: WebShop application: use case diagram

8. **Bob accesses the WebTravel application**

   Bob recalls that he needs hotel and flight reservation for a business trip. He then accesses the WebTravel service (while still logged into the Portal, in a seamless way) and he makes his hotel and flight reservation selecting his trip details.

9. **Bob is asked to authorize the automatic compilation of the reservation form**

   In order to complete the hotel reservation, an electronic form must be filled with personal data. The system detects, through the presence information, that Bob is currently using a smartphone so, in order to help him to fill the form, Bob is asked to give this authorization for the automatic compilation of the reservation form.

10. **Bob accepts the automatic compilation of the reservation form**

    Bob accepts and allows the retrieval of this information from the IdP in a secure manner.

11. **Automatic completion of the form is carried out**

    WebTravel accesses only needed information from the IdP by using a secure communication protocol. After received, WebTravel completes the form for Bob.

Actors and their interactions with the WebTravel application described in steps 8-11 are represented in the use case diagram in Figure 8.

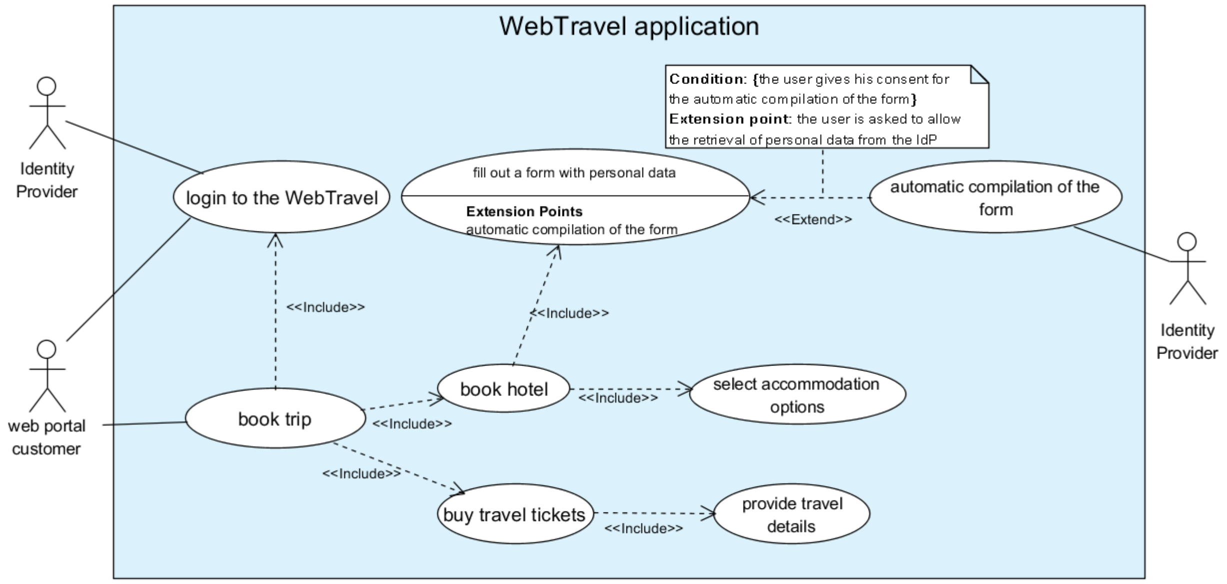

WebTravel application
Condition: {the user gives his consent for the automatic compilation of the form}
Extension point: the user is asked to allow the retrieval of personal data from the IdP
Identity Provider
login to the WebTravel
fill out a form with personal data
Extension Points
automatic compilation of the form
<<Extend>>
automatic compilation of the form
Identity Provider
<<Include>>
<<Include>>
web portal customer
book trip
book hotel
<<Include>>
select accommodation options
<<Include>>
<<Include>>
buy travel tickets
<<Include>>
provide travel details

Figure 8: WebTravel application: use case diagram

3 Case study B: “The emerging European Air Traffic Management systems”

3.1 Introduction

The European airspace is fragmented and congested. Air navigation services and their supporting systems are not fully integrated, and are based on technologies already running at their max. To cope with this congestion, early this century, it was thought that a “paradigm shift” (i.e. a breakthrough) was required. This led to the creation of the Single European Sky ATM Research (SESAR) Programme. The SESAR Joint Undertaking (JU) was created under European Community law, to manage the SESAR Development Phase.

During the recent years, a new operational concept (CONOPS) was developed for ATM. One of the main identified operational enablers is the System Wide Information Management (SWIM). SWIM is a distributed processing environment, which replaces data level interoperability and closely coupled interfaces with an open, flexible, modular and secure data architecture totally transparent to users and their applications. SWIM will be of course open to all traditional ATM stakeholders & systems. However, it is also foreseen to be open to non-traditional ATM stakeholders, thus given birth to new & strong security needs in a domain that has always focused exclusively on safety. A glossary that clarifies terms used in ATM domain can be found in Appendix A.1.

3.1.1 Scope

There are currently different scopes to what people understand by SWIM.

The 1st vision is a full-fledged operational view, i.e. a system of systems, allowing for a common virtual information pool to replace point-to-point communication between all ATM stakeholders, as pictured below.

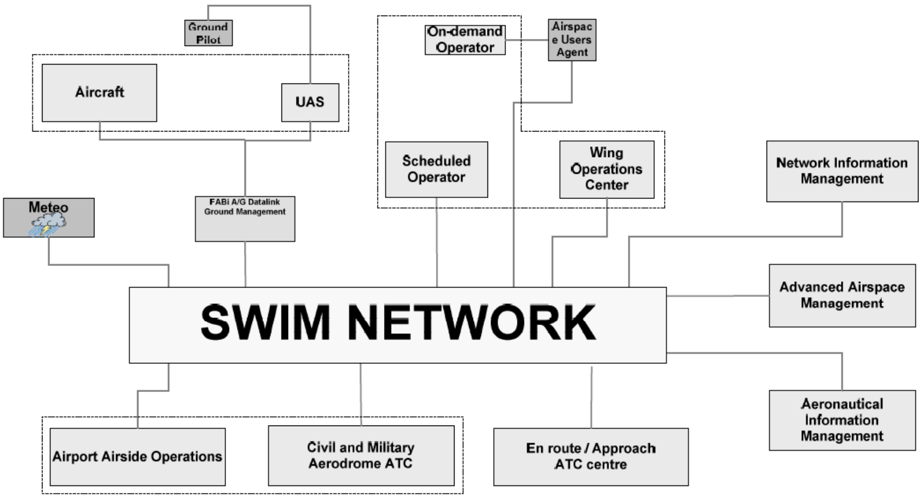

Ground Pilot
On-demand Operator
Airspace Users Agent
Aircraft
UAS
Scheduled Operator
Wing Operations Center
Network Information Management
Meteo
FABi A/G Datalink Ground Management
SWIM NETWORK
Advanced Airspace Management
Aeronautical Information Management
Airport Airside Operations
Civil and Military Aerodrome ATC
En route / Approach ATC centre

Figure 9: Hypothesis 1, full-fledged SWIM operational view

In this view, the SWIM environment expects at least the following data to be shared: flight data, surveillance data, aeronautical data, meteorological data, capacity and demand data, air traffic flow management (ATFM) scenario data.

The 2nd vision is a domain-agnostic information management view. In this vision, cf. figure below, SWIM has a much more limited scope and two different interfaces are defined, based on ICOG middleware ICD definitions. This is the currently prevailing vision and the one we intend to develop in Aniketos.

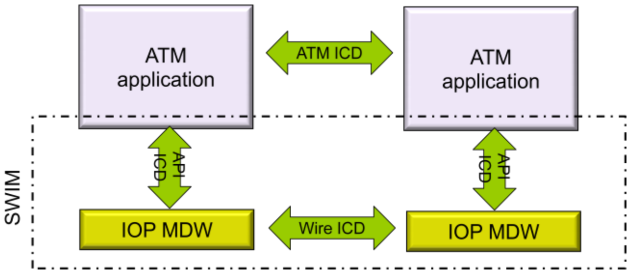


Figure 10: Hypothesis 2, domain-agnostic information management view

This view is also called the “payload approach”, because the ATM application builds the payload, invokes (via the application interface - API ICD) the interoperability middleware (IOP-MDW) to send the payload containing the packed events or services to the proper destination. The IOP-MDW distributes the payload to another instance of the IOP-MDW in the destination system.

The EUROCAE ED-133 standard provides a typical example with the Flight Object (FO) interoperability specification (see figure below).

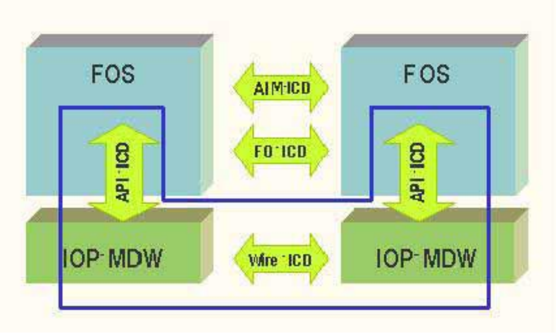


Figure 11: Two Flight Object Servers on a SWIM infrastructure

In this example, a client Flight Object Server (FOS) wants to set a constraint on a flight plan held by another FOS. This is pictured by a “SetConstraint” interface in the Flight Object Interface Control Document (FO-ICD). In reality, the service is rendered by composing different services to send this request as a “payload” through the IOP-MDW (cf. picture below).

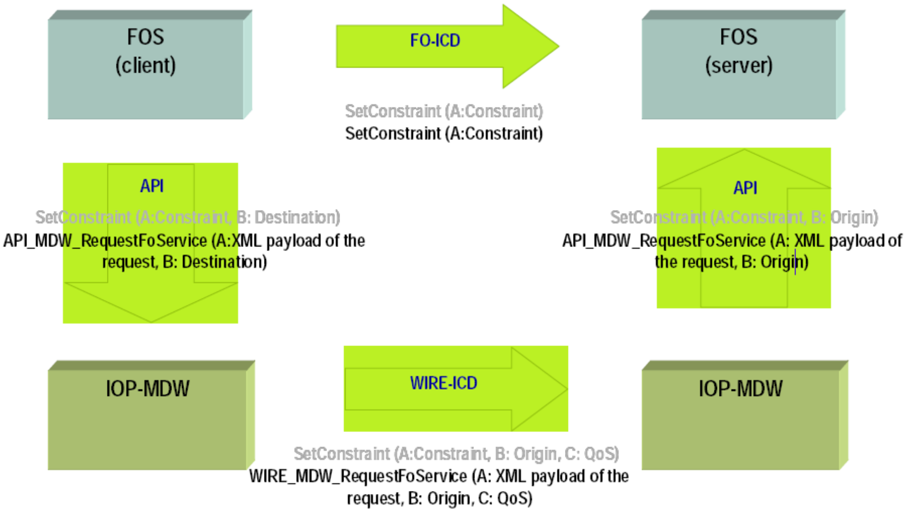

FOS
(client)
FO-ICD
FOS
(server)
SetConstraint (A:Constraint)
SetConstraint (A:Constraint)
API
SetConstraint (A:Constraint, B: Destination)
API_MDW_RequestFoService (A:XML payload of the request, B: Destination)
API
SetConstraint (A:Constraint, B: Origin)
API_MDW_RequestFoService (A: XML payload of the request, B: Origin)
IOP-MDW
WIRE-ICD
IOP-MDW
SetConstraint (A:Constraint, B: Origin, C: QoS)
WIRE_MDW_RequestFoService (A: XML payload of the request, B: Origin, C: QoS)

Figure 12: The “set constraint” example between Flight Object Servers

One problem in defining SWIM is that it is not as easy as it seems to choose between the two aforementioned visions, i.e. the full-fledged SWIM operational view, and the domain-agnostic information management view.

Indeed, beyond the simple request/reply & publish/subscribe interaction patterns, other patterns may arise. In particular, ED-133 recalls that the ATC system in charge of managing the Flight Object (FO) is not always the same. As the flight crosses Areas of Responsibility (AORs), the responsibility of updating the FO belongs to the ATC system in charge of the crossed area (cf. the two figures below).

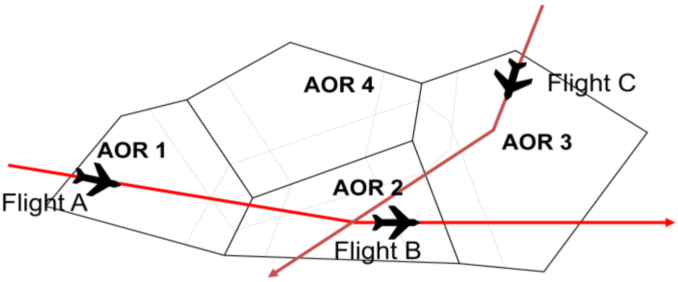


Figure 13: Example of three flights crossing three sectors

Thus, the SWIM interoperability middleware needs to know at all times where to address its payload, even when the Flight Object Server in charge of a flight plan is changing, and this transparently for the end user.

Additionally, the SWIM interoperability middleware may need to guarantee the right sequence of operations.

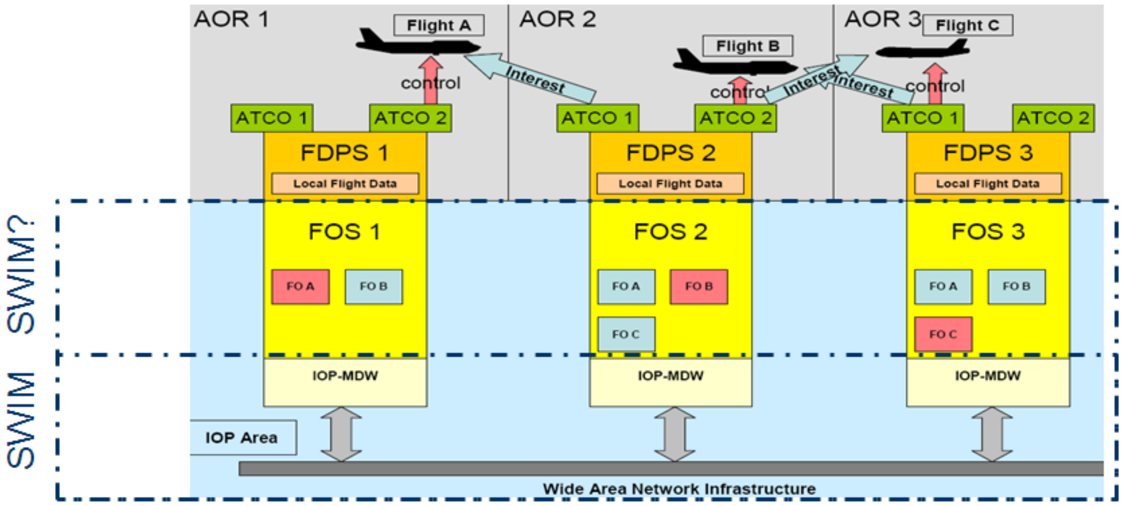


Figure 14: Logical view on the three flights crossing three sectors example

With this configuration in mind, setting the frontier of the SWIM system is not obvious (cf. picture above). We will probably need to wait for recommendations from the SESAR project on this particular issue.

3.1.2 A few architectural considerations

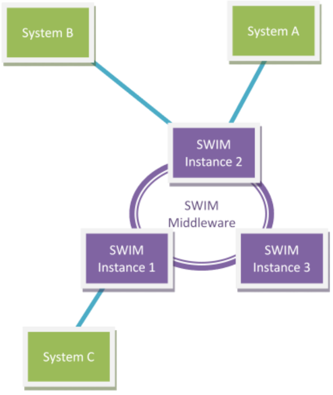


Figure 15: The SWIM MDW infrastructure

SWIM is not a single point of failure, because there is no single SWIM middleware infrastructure. The SWIM middleware is composed of many instances (cf. Figure 15).

The network supporting the SWIM middleware will be a wide area network (WAN) called the Pan European Network Service (PENS). PENS is a joint EUROCONTROL - ANSP led initiative to provide a common IP based network service across the European region covering voice and data communication and providing efficient support to existing services and new requirements that are emerging from future ATM concepts.

PENS is a fully meshed IP network. It can be considered as a private network. This has not always been the case, and this has of course direct consequences on the SWIM security requirements; one of the consequences of PENS is that the risk assessment made in the SWIMSUIT project (prior to PENS) is largely obsolete, even though PENS cannot always be assumed. Indeed, for some parts of the network, SESAR SWIM will also need to be able to run over the “normal” internet.

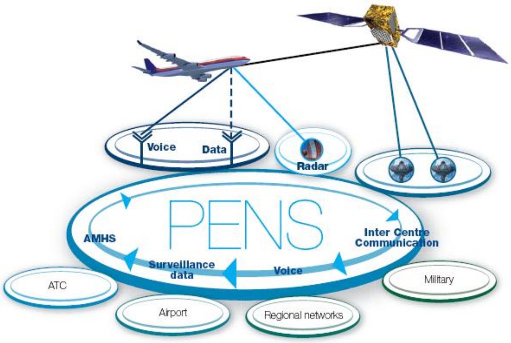


Figure 16: The PENS approach

3.1.3 Focus for the Aniketos case-study

From the above presentation, it is clear that the SWIM use-case represents a huge complexity, offering numerous opportunities to tackle scientific and technical issues. Within Aniketos, it will not be possible to analyse the whole SWIM in depth. There are two ways to scope down the analysis:

- the 1st way consists in focusing on a few applications and/or data types (e.g. flight data), so as to perform an in-depth analysis of these applications with respect to SWIM;
- the 2nd way consists in limiting the analysis of each application using SWIM to a gross analysis, keeping the overall analysis shallow in depth, but large in extent (i.e. similar to SWIM-SUIT).

The definition of the perimeter of the study has not yet been performed. However, this definition is a mandatory step of the socio-technical modelling methodology. Thus, the precise definition of the Aniketos SWIM use-case scope will be defined while running the use-case.

The above reduction of the study perimeter still leaves a scope beyond the analysis capabilities and the evaluation needs of Aniketos. For Aniketos, based on a selection of current SESAR issues, it was additionally decided to put a focus on:

- Governance in a system of systems environment:
  - Establishment of a governance framework,
  - Processes to determine who is empowered to make certain decisions,
  - Mechanisms and policies to measure and control the way those decisions are implemented;
- Core business services.

Related to governance, the scope that can be covered in Aniketos is:

- Identification and description of stakeholders & social structures;

- Definition of policies, with an obvious focus on security policies.

Related to SWIM core business services, it is a priori possible to split them in 4 categories:

- Services offered to ATM service providers:
  - Service registering / upgrade / retirement;
  - Service publishing;
  - Service reply;
- Services offered to ATM service consumers:
  - Service subscription / un-subscription;
  - Service request;
- Services offered to the SWIM governance:
  - Add / remove a new node;
  - Maintenance on a node;
- Other (transverse) services:
  - Security services;
  - Monitoring services;
  - Logging services;
  - Configuration services;
  - Testing services, etc.

3.1.4 Design-time restriction

Compared to the two other Aniketos use-cases, SWIM use-case is restricted to design-time validation. The reasons behind this decision are as follows:

- SWIM is a very complex system of systems use-case which would be very difficult to prototype, especially considering the scheduled effort on this case-study (according to the DOW);
- the SWIM concept is not yet completely specified by its stakeholders;
- very interesting results can be achieved on this use-case in relation to design-time tools.

The consequence of this “design-time” restriction is that the ANIKETOS validation (WP7) on this use-case is restricted to the application of the ANIKETOS design time tools to the use-case modelling, including requirement engineering, socio-technical modelling, security risk assessment, etc.

3.1.5 Relevance to Aniketos

ATM is a typical safety-critical domain. In this context, SWIM pictures some obvious security needs, mainly:

- Integrity, at least related to the following aspects:
  - Authentication: (i) a service consumer has to be authenticated before using SWIM; (ii) SWIM has to authenticate itself when invoking the service provider; and (iii) the SWIM instances need to authenticate between each other;
  - Authorization: a service consumer needs to be authorized to invoke a service provider.
- Confidentiality: (i) at design-time, confidentiality needs to be insured between service providers; (ii) at run-time, confidentiality needs to be insured between the service consumers and their service providers.

Specific security needs related to SWIM availability are a little bit less obvious, as availability may be related to PENS and a large part of availability concerns is already covered by safety considerations.

For more details related to security needs, please refer to §3.2

3.1.6 Benefits expected from the Aniketos results

Benefits are expected at project / consortium level, and at European level.

At project / consortium level, being a design-time only use-case, the SWIM use-case will be very demanding on the Aniketos design-time tools, especially the socio-technical modelling language. Design-time evaluation results on SWIM should therefore be highly relevant.

At European level, the benefits will depend on the level on interaction with the SESAR SWIM and Security work-packages. Intellectual Property Rights (IPR) issues are currently being discussed between the Aniketos consortium and the SESAR JU. When these IPR issues are solved:

- Aniketos will be able to present its approach (i.e. methodology and tools);
- SESAR will be able to expose its security-related challenges in detail;
- Aniketos will be able to address those challenges using the Aniketos approach, and present its results.

3.2 Security and trustworthiness problems

A common European ATM system will be a huge distributed information system and a cornerstone of European Critical Information Infrastructure. As such it will be both difficult to master its security, and a tempting target for hackers.

3.2.1 Baseline

The SWIM-SUIT project [1] identified a number of threats to the following ATM assets:

- SWIM data: flight data (FD), surveillance data (SD), aeronautical data (AD), capacity and demand data (CD), ATFCM scenario data (AT), meteorological data (MT), AOC data (AO);
- SWIM SW/MDW (SM): it includes operational software, and network data and software;
  - the operational software typically includes middleware for implementation of publish / subscribe and request / reply paradigms, database engines, with proper replication agents and managers for synchronization and geographical organization of data, wrappers for integration of legacy systems within SWIM, a variety of clients to fulfil access to the SWIM infrastructure, etc.;
  - the network data and software typically includes software for implementation of routing functionality on the ground-ground and on the air-ground segments; software for interconnection with legacy networks, e.g. ATN and ACARS, software/firmware for new wide-band air-ground data link implementation for en-route / approach, software/firmware for new wide-band air-ground data link implementation for airports, software for implementing aircraft handoff between the two data links in gate to gate operation, configuration data for ground-ground segments: addressing and routing tables; configuration data for air-ground segments: addressing, routing tables and location registers; software for implementation of firewalls and security-oriented protocols, e.g. SSL, IPSEC, etc., software for implementation of public key infrastructures (if any), certificates, username & passwords, private keys, etc.;
- SWIM technical system (TS) for network management: it includes all software packages and related data that are the building blocks for fault and configuration management, redundancy handling or recovery procedures, performance management, user profiles administration, data logging and recording;

The lists above are not exhaustive, but are representative of the asset classes.

The threats related to these assets (cf. Table 4) are numbered with the asset abbreviation as specified above (e.g. FD1 for the first threat relevant for flight data). Information is copied from the SWIM-SUIT deliverable.

Number	Threat description	Comments/Explanation
FD1	Denial of Service during Taxiing phase	Updated data not available for Surface Movement Management and Runway Usage Management System Users towards the airplane(s) and/or ATCOs
FD2	Denial of Service during Take-off	Updated data not available for Flight Data Processing System User, towards the airplane(s) and/or ATCOs.
FD3	Denial Of Service during En-Route and Approach	Updated data not available to aircraft for Flight Data Processing and Arrival Management subsystems
FD4/FD9	Message content modification by Masquerading as a Publisher OR Spoofing of an aircraft on a fake SWIM-SUIT infrastructure –{Taxiing, Pre- Flight} Phase	An attacker obtains Publishing privileges masquerading as an authorized System User. Fake Departure and Runway usage managers can compromise data integrity
FD5/FD6	Message content modification by Masquerading a Publisher OR Spoofing of an aircraft on a fake SWIM-SUIT infrastructure – {Takeoff (FD5), En-Route and Approach (FD6)} phases	An attacker obtains Publishing privileges masquerading itself as an authorized System User. Fake FDP {and Arrival Managers**}** can compromise data integrity
FD7	Message content modification of Flight data on several aircraft departing and arriving the same aerodrome	Fake data distributed to Flight Data Processing System User, towards the airplane(s) and/or ATCOs
FD8	Denial of Service during Pre-Flight phase	It is not possible to get SBTs/RBTs into SWIMSUIT
SD1	Denial of Service during Taxiing phase	Updated data not available for the following System Users: • Ground Surveillance; • Surface Movement Management towards the airplane(s) and/or ATCOs
SD2	Denial Of Service during En- Route and Approach	Updated data not available to aircraft for Ground Surveillance System User
SD3	Message content modification by Masquerading a Publisher OR Spoofing of an aircraft on a fake SWIM-SUIT infrastructure – Taxiing phase	An attacker obtains Publishing privileges masquerading as an authorized System User. Fake Ground Surveillance and Surface Movement managers can compromise surveillance data integrity
SD4	Message content modification by Masquerading a Publisher OR Spoofing of an aircraft on a fake SWIM-SUIT infrastructure – En-Route and Approach phases	An attacker obtains Publishing privileges masquerading as an authorized System User. Fake Ground Surveillance manager can compromise surveillance data integrity
SD5	Surveillance Data Eavesdropping for aircraft attack	An attacker is able to track precisely the position of one or several aircrafts even the short term planned trajectory.
AD1/2/3	Denial of Service during {Taxiing, Takeoff, En-Route and Approach} phase	Updated data not available for Aeronautical Information Management System User(s) towards the airplane(s) and/or ATCOs
AD4	Message content modification by Masquerading a Publisher OR Spoofing of an aircraft on a fake SWIM-SUIT infrastructure – Taxiing phase	An attacker obtains Publishing privileges masquerading itself as an authorized System User. Fake Aeronautical Information Manager can compromise data integrity
AD5/AD6	Message content modification by Masquerading as a Publisher OR Spoofing of an aircraft on a fake SWIM-SUIT infrastructure – {Takeoff phase, En-Route and Approach phases}	An attacker obtains Publishing privileges masquerading itself as an authorized System User. Fake Aeronautical Information Manager can compromise integrity of data used by the airplane(s)

Number	Threat description	Comments/Explanation
CD1/AT2	Denial of service	Updated data not available from the relevant Publishers, which are: • Local and sub-regional Traffic demand / Traffic flow; • Airport /Aerodrome demand and capacity; • ATFCM Scenario Mgmt • ASM scenario management. • Direct victims are AOC, en-route/approach and aerodrome systems. Aircraft too, but not directly.
CD2/AT2	Message content modification by Masquerading as a Publisher OR Spoofing of a system/subsystem on a fake SWIM-SUIT infrastructure	An attacker obtains Publishing privileges masquerading itself as an authorized System User in order to compromise data integrity
MT1/MT2	Denial Of Service during {Takeoff (MT1), En-Route and Approach (MT2)}	Updated data not available for IOP/SWIM-SUIT mgmt, towards the airplane(s) and/or ATCOs
MT3/MT4	Message content modification by Masquerading as a Publisher OR Spoofing of an aircraft on a fake SWIM- SUIT infrastructure – {Takeoff phase (MT3)[1], En-Route and Approach phases (MT4)}	An attacker obtains Publishing privileges masquerading itself as an authorized System User. Fake IOP manager can compromise integrity of data used by the airplane(s)
TS1	Denial of Service of the SWIMSUIT Supervision system	An Attacker compromises the Supervision systems: • Stop ATM services • Stop Infrastructure services (including the security service itself)
TS2	Message content modification by Masquerading the Supervision System	An Attacker compromises the Supervision systems, by: • Modifying Infrastructure services (including the security service itself) • Suppressing alert messages destined for the SWIM-SUIT manager (e.g. security alerts) • Compromises the data recording mechanisms (hence hiding his own presence after the attack)
TS3	Message content modification by directly accessing the SWIM Virtual Information Pool	An Attacker gains a direct access to the SWIM Virtual Information Pool and compromises data integrity
AO1	Eavesdropping of sensitive data	An attacker can “read” AOC and security data from the SWIM
SM1	Denial of Service of SWIM ATM data	An attacker uses some security weakness or flaw in the Software or Middleware to stop ATM services, partly or fully
SM2	Message Content modification of SWIM ATM data	An attacker uses some security weakness or flaw in the Software or Middleware to compromise the ATM virtual information pool data integrity

Table 4: Threats identified by the SWIM-SUIT project

The SWIM-SUIT project performed a risk analysis of these threats, which can be summarized as follows:

[1] To the best of our knowledge, no meteo data is exchanged during takeoff, so this threat is irrelevant.

Moderate risks: FD6, FD7, FD9, SD4, AD5, AD6, CD2, AT2.

High risks: FD3, SD5, CD1, MT4, TS1, TS2, TS3, AO1, SM1, SM2.

To conclude, it should be said that the risk analysis performed by SWIM-SUIT may no longer be relevant due to changing technology and/or assumptions. Aniketos will perform the risk assessment anew, but limiting itself to a much smaller perimeter. It will however be interesting to compare the results, and possibly also the methodological approaches.

3.2.2 Aniketos scope

Within the Aniketos project, the socio-technical modelling language (cf. D1.3 and D1.4) and some other project baseline tools (e.g. the Thales risk assessment domain specific modelling language) allow for the specification of security needs and system security requirements. For the SWIM use-case, we will be using these tools to model the domain and elicit the security needs and security requirements, as part of the work in WP6 and WP7. The threats listed above and the domain requirements as listed in §3.7.1 represent a consistent baseline with which to compare the results we will obtain using the Aniketos methodology and design-time tools. Depending on the results, this work may be complemented with an analysis of possible countermeasures to be adopted, techniques to prevent such threats and explanation of the reasons that may generate them.

3.3 Analysis of existing solutions

Due to unresolved SESAR IPR issues, we can only consider solutions specified by the SWIM-SUIT project at this time. To the best of our knowledge[2], none of the security mechanisms identified by SWIM-SUIT were actually implemented in the prototype.

SESAR has identified various general SOA security solutions, but it has not yet been determined to what extent they are applicable to SWIM. SESAR SWIM is currently not considering composable services.

3.4 Users definition

The SWIM stakeholders are all the people and organizations that are involved in Air Traffic Management. We can differentiate two types of stakeholders (as outlined by the OASIS SOA approach) that are the SWIM participants versus the SWIM non participants.

The SWIM non participants are legal authorities, aeronautical standardization bodies and tax collecting organizations. The legal authorities are those organizations that publish legislation applying to the SWIM environment; within the European Union, we can identify the European Union itself, the EU member states and to a certain extent the non-EU member states that have specific agreements with the EU. The aeronautical standardization bodies are ICAO at the worldwide level and EC at the European level. The tax collecting organizations are EC (on behalf of EU member states) and aerodromes.

The SWIM participants are those organizations involved in the preparation and execution of the flights, i.e. airlines and other airspace users operating the flights, ANSPs, airports and military organizations operating the air traffic control, industries providing systems interoperating with the SWIM.

Any stakeholder may act as a participant and non-participant at the same time: a good example is EUROCONTROL, who acts as a standardization body, as a tax collecting organization and as Air Traffic Flow Management (ATFM) organization.

[2] Based on information from the first SWIM-SUIT user forum, December 2009.

3.4.1 Aircraft

Role

In the SESAR Operational Concept aircraft are travelling nodes in the SWIM network, permanently connected by high capacity air/ground data link.

Using the SWIM, aircraft will become both consumer and producer of information, which they will share with the other SWIM users.

3.4.2 Aircraft Operator

Role

An Aircraft Operator is a person, organization or enterprise engaged in or offering to engage in an aircraft operation.

3.4.3 Airport operator

Role

Herein we are interested only by the Airport Airside Operations. Within this scope, the Airport Operator is responsible for aerodrome operations such as the management of aircraft de-icing, and aircraft turn-round (stand / gate allocation, ground handling…)

3.4.4 Air Traffic Control Unit (TWR, APP, ACC or UAC)

Role

Air traffic control units are specialised in providing air traffic control services, but they are also responsible for flight information service (FIS) and alerting service to pilots (i.e. assisting aircraft in difficulty and initiating search and rescue).

An air traffic control unit is typically responsible for: (i) aerodrome control service, in which case it is called the aerodrome control tower (TWR); (ii) approach control service, in which case it is called the approach control unit (APP); (iii) area control service, in which case it is called the area control centre (ACC) or upper area control centre (UAC).

3.4.5 Air Traffic Service Unit (ATSU)

Role

An air traffic service unit (ATSU) is a unit established for the purpose of receiving reports concerning air traffic services and flight plans submitted before departure. Such a reporting office may be established as a separate unit or combined with an existing unit. It is a generic term meaning air traffic control unit, flight information centre, or air traffic service reporting office.

3.4.6 MET provider

Role

Meteorological services are facilities and services that furnish aviation with meteorological forecasts, briefs and observations as well as SIGMET information (i.e. information issued by a meteorological watch office concerning the occurrence or expected occurrence of specified en-route weather phenomena which may affect the safety of aircraft operations), VOLMET (i.e. meteorological information for aircraft in flight) broadcasting material and any other meteorological data provided by States for aeronautical use.

3.4.7 EUROCONTROL

Role

EUROCONTROL plays many roles within the SWIM ecosystem: it is a non-participant as being a provider of regulatory rules, of aeronautical standards and as performing the tax collecting on behalf of EC member states. In addition EUROCONTROL plays a participant role as operating the CFMU in charge of air traffic flow management (ATFM) for the European airspace. EUROCONTROL also performs the air traffic control for upper airspace (UAC) at Maastricht.

3.4.8 Complementary roles

Air Navigation Service Provider (ANSP)

Role

The air navigation service provider is the authority directly responsible for providing both visual and non-visual aids to navigation within a specific airspace in compliance with, but not limited to, ICAO rules and, other international, multi-national, and national policy, agreements or regulations.

AIS provider

Role

Aeronautical information service (AIS) is a service provided for the collection and dissemination of information needed to ensure the safety, regularity and efficiency of air navigation. Such information includes the availability of air navigation facilities and services and the procedures associated with them, and must be provided to flight operations personnel and services responsible for flight information services (FIS).

Civil Aviation Authority (CAA)

Role

The governmental entity or entities, however titled, that are directly responsible for the regulation of all aspects of civil air transport, technical (i.e. air navigation and aviation safety) and economic (i.e. the commercial aspects of air transport). [ICAO]

Commercial Operator

Role

An operator that, for remuneration, provides scheduled or non-scheduled air transport services to the public for the carriage of passengers, mail or cargo. This category also includes small-scale operators, such as air taxi operators, that provide commercial air transport services. [ICAO]

European Union (EU)

Role

The European Union acts as an international regulator.

General Aviation (GA)

Role

Community comprising Business Aviation (BA), High-End GA (IFR or mixed IFR/VFR flights), Low-End GA (VFR only), VLJ Operators, IFR Helicopter Operators, factory demonstrations and flight trials etc.

General Air Traffic (GAT)

Role

General Air Traffic is defined as all flights which are conducted in accordance with the rules and procedures of ICAO and/or the national civil aviation regulations and legislation.

Civil flights usually come under the category of general air traffic (GAT: IFR or VFR), but GAT may also include some military traffic.

ICAO

Role

ICAO is a specialized agency of the United Nations that codifies the principles and techniques of international air navigation and fosters the planning and development of international air transport. It acts as a standardization body and international regulator.

Industry

Role

Industry may play a wide variety of roles, as a solution provider or as a service provider.

Military

Role

Military organizations play multiple roles: e.g. military aircraft operator, ANSP when performing ATC for an airspace or airport, airport operator when managing a military or civil/military airport.

Operational Air Traffic (OAT)

Role

Operational Air Traffic is defined as all flights which do not comply with the provisions stated for General Air Traffic (GAT) and for which rules and procedures have been specified by appropriate national authorities.

OAT typically includes both military operations traffic and acceptance / test flights.

PEN Service Steering Group (PSSG)

Role

The PEN Service Steering Group (PSSG) represents the PENS users, which would set policy and standards and review performance.

PENS User Group (PUG)

Role

The PENS User Group (PUG) consists of members from the user community, which provides technical, financial and administrative advice to the PSSG.

PENS Management Unit (PMU)

Role

The PENS Management Unit (PMU) implements the policy and standards set by the PSSG, and manages the PEN Service.

States

Role

The regulatory function remains the responsibility of the European Union States and can be exercised by Government and/or independent safety, airspace and economic regulators depending on the national institutional arrangements. Often there is a division between the regulator or civil aviation authority (CAA) and the air navigation service provider (ANSP).

The role is the same for non-EU States, but outside EU rules.

UAV/UAS

Role

An Unmanned Aircraft System (UAS) comprises individual 'System elements' consisting of the unmanned aircraft (UA), the Pilot Station and any other System Elements necessary to enable flight, such as a Communication Link and Launch and Recovery Element. There may be multiple UAs, Pilot Stations or Launch and Recovery Elements within a UAS.

An Unmanned Aircraft is an aircraft which is designed to operate with no human pilot on board, as part of a UAS. Moreover a UA:

- is capable of sustained flight by aerodynamic means;
- is remotely piloted or automatically flies a pre-programmed flight profile;
- is reusable;
- is not classified as a guided weapon or similar one-shot device designed for the delivery of munitions.

The acronyms RPA and UAV may be used interchangeably, with the same meaning. [UK CAA – CAP 722]

3.5 User stories description

The innovative SESAR Operational Concept is a business trajectory based system, where airspace users, ATM partners and airports stakeholders share data to make decisions based on full knowledge of accurate up-to-date information and to negotiate, even in real time, the changes to the airplane trajectory.

The new system will have new major features, first of all the System Wide Information Management (SWIM) network, an IP based data transport network that will replace the current point to point data systems with a ground/ground communications network which connects all ATM partners; ANSPs, airports and airspace users, including the military. Aircraft become travelling nodes in the network, permanently connected by air/ground data links.

Using the SWIM network, all partners become both consumers and producers of information, which they will share, tailored to external constraints and particular stakeholders' needs. The SWIM network supports the sharing of updated and precise information, and the collaborative planning of business trajectories.

The SWIM Network is the basis for developing a new Trajectory Managed environment rather than the actual one that is based on Airspace Management. The new Trajectory Management Operational Concept is based on (i) a Collaborative Decision Making process among all air transport actors to define a rolling Network Operations Plan and to negotiate trajectory changes and (ii) an extensive use of automation support to reduce controller and pilot workload, and to enable new separation modes by taking advantage of advanced aircraft navigation capabilities.

All the above mentioned structural changes, which involve the deployment of new IT systems (e.g., new ground based and on-board decision making supporting tools, a new network connecting all the ATM actors and providing them with real time information, etc.), should enable an extraordinary evolution in the deployment and support of future ATM services. The deployment of new IT systems and their architecture are changing the nature of ATM services itself. From 'closed' and dedicated systems, ATM services are relying more and more on 'open', ubiquitous and composite systems. Hence, ATM systems are becoming vulnerable to new types of hazards due to different factors. For instance, the openness of the information systems makes them vulnerable not only to malicious exploitations but also to integrity and availability hazards. Trust problems arise between ATM stakeholders, who have to rely on mediated information.

In the following tables we will detail four User Stories, i.e., realistic Operational Scenarios of usage of the SWIM platform.

User story B1 – Meteo Service Registering and Subscription	
Description	A National Meteo Service Provider develops a new system to provide more accurate, frequent and accessible Meteo Information related to specific areas (e.g. Terminal Areas). The National Meteo Service Provider submits a service accreditation request to the SWIM Governance. The SWIM Governance formally approves the new service for deployment and operation. Thus, the National Meteo Service Provider makes available additional Meteo Information related to the Terminal Area of a big European hub. This service is of interest to all the air carriers using this hub that decide to subscribe to the new service immediately. Moreover, also the Airport Operation Centre (APOC) of the hub subscribes to the new upgraded service.
Involved roles	National Meteo Service Provider SWIM Governance Air Carriers Airport Operation Centre(s)(APOC)
Outcome	User Story B1 presents the secure and trusted environment for the following operations: 1) an organisation wants to provide a new service on the SWIM: service registering and 2) an organisation wants to use a service for the 1st time: service subscription

Table 5: Case study B - User story B1

User story B2 - Meteo Information Request	
Description	Let us consider an arriving aircraft. The scenario begins when the aircraft is flying en route under the responsibility of ATSU 1 at approximately 40 minutes from touch-down. At this point, the aircraft is cleared to proceed with its agreed RBT until terminal area entry, i.e. the RBT segment within ATSU 1's AoR has been authorized. It is assumed that, to support arrival operations an updated preferred RBT from its current position to the runway based on the latest meteo information will be computed and proposes it to ATSU 1 and ATSU 2 as a revision to a segment of RBT that extends across both ATSU 1's and ATSU 2's AoRs. Main steps are: • FO Manager (Aircraft) requests latest meteo info from meteo info service and computes updated RBT segment. • FO Manager (Aircraft) downlinks updated RBT segment to FO Subscribers (ATSU1 and ATSU2). • FO Contributor (ATSU 1) retrieves RBT proposal from FO

	Manager’s (Aircraft) FO and checks it for conflicts • ATSU 2 includes constraints on FO Manager’s proposed RBT. • FO Manager (Aircraft) synthesizes new RBT segment that complies with the constraints and downlinks the new RBT segment to the FO Subscribers (ATSU 1 and ATSU2).
Involved roles	ATSU 1 ATSU 2 Aircraft SWIM Network
Outcome	User Story B2 presents the secure and trusted environment for the following operations: 1. Meteo Service Information Request; 2. Meteo Service Information Provision; 3. RBT update, 4. SWIM manages one request/reply service: R/R service operation; 5. SWIM manages one publish/subscribe: P/S service operation.

Table 6: Case study B - User story B2

User story B3 – AMAN Retrieves RBT Information	
Description	The scenario involves *N* aircraft (A/C) scheduled to land in an airport *A* during a given time interval *T* (an arrival flow into airport *A*), together with two Air Traffic Service Units: ATSU 1 (Area Control Centre - ACC), which is responsible for controlling the *N* aircraft as they transition from the en route phase of flight into the terminal area around airport *A*, and ATSU 2 (Approach - APP), which is responsible for controlling the *N* aircraft within the terminal area. It is assumed that ATSU 2 is supported by an Arrival Manager (AMAN) tool with a horizon that extends to include incoming aircraft up to 40 minutes before they are due to land. Thus, it is assumed that, in order to build an optimal arrival sequence, the AMAN must take into account arriving aircraft before they enter ATSU 2’s Area of Responsibility (AOR). In this scenario, this means that ATSU 2 requires surveillance and Reference Business Trajectory (RBT) information of the incoming aircraft while they are still within ATSU 1’s AOR.
Involved roles	ATSU 1 ATSU 2 Aircraft ATSU 2 Arrival Manager SWIM Network
Outcome	User Story B3 presents the secure and trusted environment for the following operations: 1. FO/RBT info retrieval ; 2. Request of AOC Info 3. FO/RBT update; 4. FO/RBT publish;

Table 7: Case study B - User story B3

User story B4 – Flight Handover	
Description	An ATM system tries to handover responsibility of a Flight (and of the corresponding FO) to another ATM System. The FO Server of ATSU1 to handover the FO (FOS1) is securely connected to the SWIM infrastructure upon authentication. FOS2 that is to receive responsibility over the FO is securely connected and it is a subscriber of the FO. SWIM provides a token for any subsequent data exchange session between the ATM system and SWIM. The Scenario starts when the FOS1 wishes to transfer responsibility over the FO to FOS2. A change of AoR is simulated from ATSU1 to ATSU2. The role is exchanged after the boundary. Main steps are: • FO Manager (FO Server 1) sends the handover request to SWIM • SWIM notifies the handover request to the identified potential FO manager (FO Server 2) • The potential FO Manger (FO Server 2) accepts handover SWIM assigns the manager role to FO Server 2.
Involved roles	ATSU 1 ATSU 2 Aircraft ATSU 1 FO Server ATSU 2 FO Server SWIM Network
Outcome	User Story B4 presents the secure and trusted environment for the following operations: 1. Flight Handover and AoR change.

Table 8: Case study B - User story B4

We recall that, being design-time only (cf. §3.1.4), the ATM use-case has a blurry frontier between WP6 (i.e. “Realisation of industry case studies”) and WP7 (i.e. “Validation and end user evaluation”). Indeed, this use-case cannot be built then validated, because the building phase itself must be validated. This implies that the building of the ATM use-case must be performed using Aniketos design-time tools, and that the evaluation must be performed in parallel to the design.

The end-users from whom evaluation results will be collected are exclusively system designers (internal and/or external to the Aniketos consortium). The modelling tasks that will be requested from them will consist mainly in:

- capturing the scenarios described above using the Aniketos design-time modelling methods and tools,
- performing a security risk assessment on the resulting architecture using the Aniketos design-time modelling methods and tools.

The evaluation objectives, evaluation methods, indicators and metrics are all defined as part of WP7. Please refer of D7.1 (i.e. “Validation and evaluation plan”) for more details.

3.6 Domain constraints

SWIM is a very large, geographically dispersed IT environment with many stakeholders and trust boundaries. Also there may be no clear definition of "outside" and "inside" because the interactions are most likely not tiered and there are probably no simple portal-style access mechanisms. Every system calls the services it requires directly through the SWIM system. It shall be therefore important to protect each node, which we will call a "self-defence approach". Each node shall decide whether to process a request or not based on a security policy. This decision needs to be enforced locally, because nodes can be owned and managed by different and heterogeneous stakeholders.

Moreover, SWIM could apply several middleware architectural approaches, including request-reply, publish-subscribe, and information-flow-centric. The SWIM middleware security architecture needs to support all of these approaches and the secure interoperability between middleware "islands". This can be achieved by multi-protocol support or gateways. Trustworthy privilege delegation across multiple different middleware islands will be technically complex but will most likely also be a requirement due to the anticipated interaction chains across trust boundaries.

Depending on the organisational structure and the type of security model, the policy can be defined and maintained centrally for the entire SWIM system, federated by each stakeholder, or decentralised by each node administrator. In the ATM domain, where European Regulatory Institutions and National Organisations interact and coexist, it is possible that system-wide regulatory policies need to be preserved in addition to locally defined policies by information providers based on their de-centralised policy.

The SWIM middleware security architecture needs to support many different types of security policies. This is both because the system (and its features) will change over time to meet new opportunities and challenges and also because SWIM will have to integrate stakeholders with very different security IT requirements, from ground handlers over civilian ATC to military ATC. In either case, security policy management needs to be supported in such a way that it is consistent and low-maintenance. For example, it would be too high maintenance if the security policy at every node in the SWIM system needs to be manually verified and, if required, updated to reflect the changes. Instead, to minimise security management costs, the SWIM middleware security policy management support needs to be able to update the security policies whenever and wherever needed with minimal human intervention.

3.7 Domain specific requirements

In this section requirements related to the ATM domain are collected.

3.7.1 Security requirements

Here is reported a list of high-level security and trust requirements for the SWIM system. They are mainly derived by means of an extensive Risk Assessment carried out in the SWIM-SUIT project [1], reviewed and refined by ATM experts working in SESAR and classified by using the Confidentiality-Integrity and Availability (CIA) properties, as proposed in Section 3.1.3.

Integrity / Authentication

Requirement ID – Type:	6B.1
Requirement Name:	SWIM Authentication
Description:	Any Contributor and Publisher must access the SWIM infrastructure upon an Authentication session. Users shall authenticate themselves for data management that require a high confidentiality degree. The SWIM Infrastructure shall authenticate itself towards the Contributor / Publisher paradigm.
Rationale:	All the actors participating in the SWIM should have access to the provided services and resources through a secure way. Depending on the role, data exchanged and confidentiality degree, the authentication mechanism might be different.

Requirement ID – Type:	6B.2
Requirement Name:	Security Mechanisms for Authentication
Description:	Proper crypto keys shall be provided after this authentication session. These keys shall be used for any subsequent data exchange session between stakeholders and SWIM. Authentication sessions based on certificates digitally signed by a trusted Certification Authority is required.
Rationale:	All the actors participating in the SWIM should have access to the provided services and resources ensuring high security and trust standards.

Requirement ID – Type:	6B. 3
Requirement Name:	Dynamic Authentication
Description:	Network components should re-authenticate every publisher that enters the network every time he does it.
Rationale:	Due to the highly dynamic ATM environment every user and transaction should be re-authenticated even if it is coming from the protected network.

Requirement ID – Type:	6B. 4
Requirement Name:	Detection of Fake Stakeholders
Description:	The SWIM Infrastructure shall be able to detect “Fake Stakeholders” and trace them in a “blacklist”.
Rationale:	In order to prevent malicious attacks and data spoiling SWIM shall be able to detect “Fake Stakeholders”.

Integrity / Authorization

Requirement ID – Type:	6B. 5
Requirement Name:	Security Auditing
Description:	Proper measures shall be taken in order to select SWIM software and middleware that has been passed security auditing sessions.
Rationale:	The SWIM Governance is in charge to periodically audit and select proper software and middleware solution to ensure a high security and trust level in the whole Network.

Requirement ID – Type:	6B. 6
Requirement Name:	Authorization and Privilege Management
Description:	Stakeholders must demonstrate that they can be granted their privileges. This should be made before the authentication phase. Stakeholder privileges are defined by “administrator entities”. Change of privileges must be made and agreed between the various administrators of each data.
Rationale:	The SWIM Governance is in charge to periodically audit SWIM stakeholders to ensure a high security and trust level in the whole Network.

Requirement ID – Type:	6B. 7
Requirement Name:	Dynamic Authorization
Description:	Network components should re-authorize every publisher that enters the network every time he does it. Every transaction should be re-authorized even if it is coming from the protected network.
Rationale:	Due to the highly dynamic ATM environment every user and transaction should be re-authorized even if it is coming from the protected network.

Confidentiality

Requirement ID – Type:	6B. 8
Requirement Name:	Data Encryption
Description:	Any sensitive data (e.g. AOC) and, in particular, surveillance data shall be encrypted.
Rationale:	In order to ensure confidentiality and integrity of sensible data, preventing their corruption, accidental or intentional loss, proper encryption mechanisms shall be put in place.

Availability

Requirement ID – Type:	6B. 9
Requirement Name:	Data Availability Mechanisms
Description:	Flight data, Capacity & Demand Data and SWIM Supervision System data shall be supported by: • Redundant communication infrastructure; • Air-Ground data link diversity; • Multiple access nodes; • Back-up solutions for data storage.
Rationale:	The provisioning of information regarding SWIM sensitive data by specific actors and systems must be guaranteed 24 hours a day, 7 days a week.

3.7.2 Technological requirements

As expressed in §3.1.4, this use-case is restricted to design-time validation: this section is therefore non-applicable.

3.7.3 Run-time requirements

As expressed in §3.1.4, this use-case is restricted to design-time validation: this section is therefore non-applicable.

3.8 Storyboard

The storyboard lists the exact sequence of actions carried out by the users involved in the case study. It represents what will be shown with the realization of the case study.

Storyboard derived from User Story B1:

1. The National Meteo Service Provider submits a service accreditation request to the SWIM Governance.
2. The SWIM Governance formally approves the new service for deployment and operation.
3. The National Meteo Service Provider deploys the new Meteo Information Service.

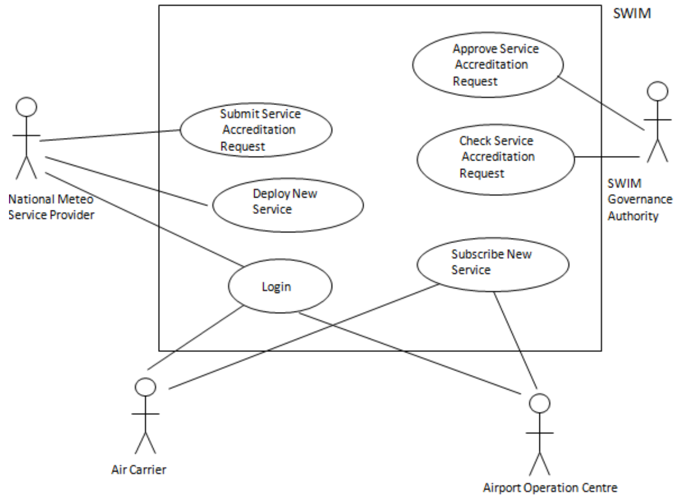

SWIM
Approve Service Accreditation Request
Submit Service Accreditation Request
Check Service Accreditation Request
Deploy New Service
National Meteo Service Provider
SWIM Governance Authority
Subscribe New Service
Login
Air Carrier
Airport Operation Centre

Figure 17: Use-case diagram for User Story B1

Storyboard derived from User Story B2:

1. A/C Subscribes to Meteo Information
2. A/C requests latest Meteo Information from Meteo Information Service Provider and computes a consequently updated RBT segment.
3. FO Contributor (ATSU 1) retrieves RBT proposal from FO Manager's (Aircraft) FO and checks it for conflicts
4. ATSU 2 includes constraints on FO Manager's proposed RBT.
5. FO Manager (Aircraft) synthesizes new RBT segment that complies with the constraints and downlinks the new RBT

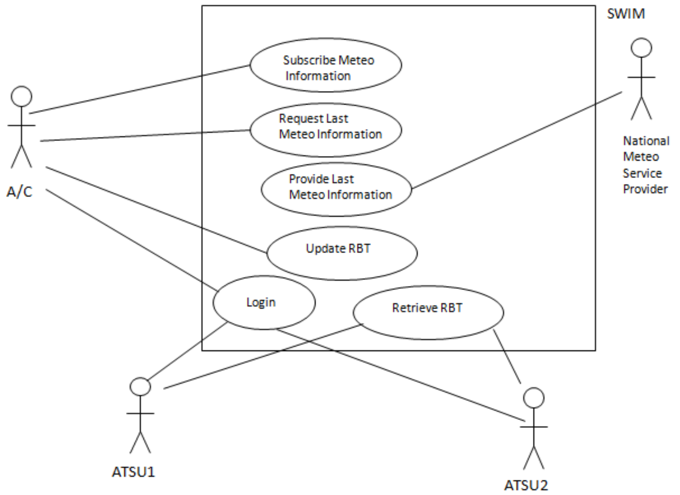

SWIM
Subscribe Meteo Information
Request Last Meteo Information
Provide Last Meteo Information
Update RBT
Login
Retrieve RBT
A/C
National Meteo Service Provider
ATSU1
ATSU2

Figure 18: Use-case diagram for User Story B2

Storyboard derived from User Story B3:

1. A/C downlinks updated RBT segment to ATSU1 and ATSU2.
2. ATSU 1 retrieves RBT proposal from AC1 and checks it for conflicts with other A/C
3. ATSU 2 AMAN retrieves RBT proposal and surveillance data and builds arrival sequence
4. A/C synthesizes new RBT segment that complies with the constraints and downlinks the new RBT segment to ATSU 1 and ATSU 2.

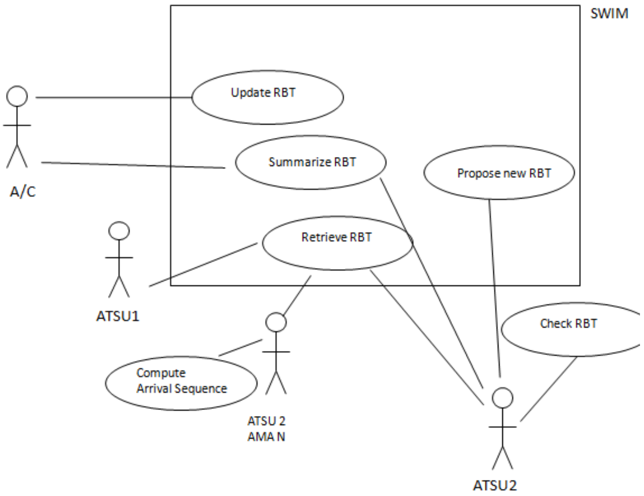


Figure 19: Use-case diagram for User Story B3

Storyboard derived from User Story B4:

1. The Flight Object Manager (the ATSU1 Server) sends the handover request to SWIM

2. SWIM notifies the handover request to the identified next potential Flight Object Manager (ATSU2 Server)
3. The potential Flight Object Manager (ATSU2 Server) accepts handover
4. SWIM assigns the manager role to the ATSU2 Flight Object Server.

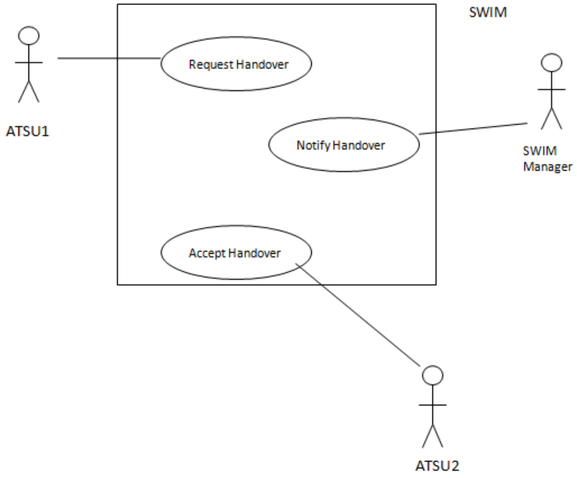


Figure 20: Use-case diagram for User Story B4

4 Case study C: "Land-buying and eGovernance"

4.1 Introduction

This case study represents a typical public service, involving multiple stakeholders, ranging from ordinary citizens to various organisations from different domains. These kinds of services are becoming more and more available online, and need to address key challenges as they are identified in Aniketos.

DAEM S.A., the City of Athens IT company, is an organisation dedicated in developing and providing e-government implementation services to local government authorities and other public organisations. The following domain specific case study represents the implementation of the supporting service framework related to the scenario of when, where and what to acquire when searching for a piece of land (lot) so as to build a residence for individual or professional use. Such a scenario involves many factors affecting decisions at various stages. In addition, many security threats and vulnerabilities are in place as a result of the nature of the e-government related scenario. Therefore, the objective identified and addressed is to enable both citizens or various service end users and different organisations interaction into a complex public service provisioning scenario.

The target outcome will be to facilitate access to the most up-to-date procedures, information on relevant regulations and advice on associated costs that affect decisions when acquiring land and issuing a respective building permit, being thus fundamental to the scenario implementation.

4.2 Security and trustworthiness problems

Security is deemed as a major strategic and technological statement to be addressed as happens in all e-government services cases. Data exchanged among the involved stakeholders should be safeguarded with respect to key security attributes, including data integrity and trustworthiness of the delivery end nodes. The current European initiative for public services is headed towards a totally new approach, in which the technological advances in the ICT domain (including the Web2.0 paradigm and the SOA-based architectures) appear to be the solution for providing accurate, secure and trusted electronic public services to citizens, enterprises and public organisations. Data involved in public services can be classified, according to their privacy level, as defined in local, national and international legislation, while the respective mechanisms for securing services may be controlled from the impact imposed by the loss of data integrity. The problem becomes more challenging as alternative end user devices and service channels are to be supported in order to improve the citizens' experience on public services and increase their satisfaction.

In this case study, vast data is exchanged to accomplish the foreseen processes for searching and managing a lot and issuing the relevant building permits as well. All this amount of data is provided by multiple information sources, ranging from public organisations and the involved end users to other external stakeholders. Based on both the European and Greek e-government interoperability frameworks, which provide the specifications and guidelines on how this public service can be electronically assembled, the relevant infrastructure should implement many interaction points and interfaces, through the realisation of secure Web services.

Security at this point spans across many attributes due to the fact that the exchanged data can be classified according to their privacy level, as it was stated above. A general classification can for instance be the following:

- Information on the lot properties, such as the geographical coordinates, the building terms that apply to the specific area that the lot resides in and other lot information are considered as data publicly available, which can be subsequently accessed by all involved stakeholders without any need for authentication.

- Lot owner information, such as the VAT number and personal ID card number, which should be securely submitted to the relevant systems in DAEM in order for the house building permit to be issued.
- If the application process for issuing the house building permit is performed over a Governmental Service Portal (GSP) and not directly from DAEM systems, the necessary trustworthiness between both the end user and the GSP, and the GSP and the DAEM system as well, should be established.

In the above described examples, we can identify two different levels of data privacy. In the first case, we deal with public data, which can be accessed by anyone, thus the services exposing such data should bear trust properties only with respect to the data accuracy. However, if a security service violation occurs and the relevant trust level is not contained, then the impact of inaccurate data on the process may not be critical.

In the second case, the data exchanged refer to private data, which should be as accurate as possible in order for the permit to be issued and access is only granted to authorised roles. In consequence, the trustworthiness of services is extended to the authenticated and role-based service access.

In the third case, a different business model is adopted by introducing the concept of a service broker that can act on behalf of the end users. The problem of security and trustworthiness in service engineering (including service design, access, execution and consumption) is further extended here to the exchange of service trust levels among multiple stakeholders.

The problem of data privacy and the relevant trust on the service provisioning becomes more critical when extending the scenario to involve bank interactions that guarantee enough resources to acquire land. In such a case, all the electronically exchanged data for calculating the credibility score and delivering the actual decision on whether the process of property management can be financially supported by the relevant financial institutions should be subject to critical decisions on the trustworthiness of the online services.

4.3 Analysis of existing solutions

Currently there has been no actual plan drafted so as to address the problem of trustworthiness in public service delivery. All existing solutions are primarily based on major human intervention when searching for a lot and delivering the house building permit. As the maturity level of this field of electronic public service appear to be low, only manual data exchange is performed, whenever a decision has to be made on the process outcome.

Existing solutions limit the scope of this scenario by enabling partial electronic access to only a subset of available data, while the rest of the process can be manually accomplished. DAEM has developed two systems that are currently running so as to facilitate selected functionalities, while other steps can be achieved through individual and ad hoc access to external third party sources. These sources may require a separate authentication mechanism. Therefore, an integrated view and implementation of this service process is a key objective to be achieved.

Current e-government practices focus on establishing of the routes for making the public service delivery a new online experience for all interacting stakeholders. Up to now, closed systems have been implemented, which may automate the processes, but they offer an isolated approach on the way data is exchanged between multiple providers. As a result, the achievement of interoperability between the existing IT systems and /or the under development ones arises as the major step to bridge the gap in existing complex e-government applications.

This key objective of integrating service delivery at the most digital level within the next few years is fully aligned with the strategic agenda for Digital Europe and the i2010 initiative. A gap has been identified as existing since current solutions only partially address the problem of authenticated access provision at the very first process steps. In addition, the absence of an integrated and fully electronic approach to this e-government scenario is more than apparent, especially in the field of trusted services, which have to be composed in order to offer the target functionalities. Therefore, Aniketos relevance and success potential in this service domain and market may be considered as predominant.

4.4 Users definition

In this section users involved in the case study are introduced, illustrating their role and what they expect from the usage of the Aniketos platform.

4.4.1 Municipality of Athens/Department of Urban Planning (DoUP)

Role

The Department of Urban Planning is responsible for the issuance of building permits. It also provides information about the building process. The DoUP will provide services that will assist the building process using the Aniketos Platform. The DoUP receives the governmental law updates and provides the relevant legislative framework including a database for the building terms. It also provides a list of the required documentation for issuing the building permit. It receives the application forms and processes the building permit application. During this process, status update of the building terms is provided.

Services offered:

- Online building permit application
- Information service of the prerequisites
- Status update service

Services consumed:

- A service to inform about law updates

Expectations: The municipality of Athens wants to offer a fast and easy option to apply for the building permit.

4.4.2 Interested party (IP)

Role

It is a party interested in the acquisition of a lot and the construction of a building upon it. The selection of the lot and of a civil engineer will be supported by services provided through the Aniketos platform. An interested party intends to buy an estate and looks for a suitable lot. Voluntarily, he can mandate a trusted real estate agent to assist his search for an appropriate object of purchase. Further counsellors (e.g. a solicitor or a civil engineer) may be required and found in online databases, where they offer their services. The purchase decision of an interested party is determined by several personal specifications. These include the purchasing price, the size, the site, the neighbourhood, or the local infrastructure. Furthermore, an interested party eventually requires additional information to make a well-informed decision. For example, these could include:

- A pricing tool can provide information about the value of the lot.
- Information about the housing area can be provided by Google earth, forums, criminal statistics
- Legal requirements have to be checked (Is the size of the lot large enough to build a house? Is it possible to get a grid connection? Who owns the trees on the land? Is the lot owner authorized to sell the lot?)

Services offered:

None

Services consumed:

- A real estate agent service
- A real estate advertisement service

- A database offering solicitor services
- A database offering civil engineer services provided by the TEE
- A pricing tool to estimate a fair value of the lot
- Internet Services providing street maps, climate information, satellite pictures etc.
- Law update services provided by the Greek Government
- A service provided by the municipality of Athens to apply for the building permit
- A creditor service

Expectations: An interested party intends to buy an estate which fits all his specifications. He expects support to make a well-informed purchase decision and a successful acquisition.

4.4.3 Lot owner

Role

A person/company owning a lot that wants to sell. The lot owner promotes its lot in an online marketplace or hires a real estate agent to sell its lot. He requires pricing information to estimate the value of its lot. He wants be assured that the buyer is able to pay the purchase price.

Services offered:

- Information about the lot (including descriptions, pictures, or maps)

Services consumed:

- A real estate agent service
- A real estate advertisement service
- A pricing tool
- A service providing a credit check of potential buyers

Expectations: The lot owner wants to sell its lot for the highest price possible and wants to be paid by the buyer.

4.4.4 Solicitor

Role

A solicitor offers his service in an online database. The interested party mandates a solicitor to supervise all legal affairs. His tasks may include to:

- Check the legal requirements
- Receive the law updates from the Government and decide how to apply them to the situation
- Run the building permit issuing process on legal terms and in cooperation with the Civil Engineer

Services offered:

- Legal advice
- Supervise the building issuing process

Services consumed:

- Law update service of the Government
- An online solicitor database to offer its service

Expectations: He wants to offer a legal advice based on the actual law status.

4.4.5 Civil Engineer (CE)

Role

An engineer certified to assist an interested party in the construction of a building. The civil engineer offers his services in an online database. He can provide information to decide which lot to buy and can support the interested party during the acquisition. His task may include

- An estimation of the value of the lot
- Identifies additional costs (e.g. for a power grid connection)
- Informs about the building terms
- Runs the building permit issuing process

Services offered:

- Pricing service
- Information about the building terms
- Supervise the building issuing process

Services consumed:

- Law update service of the Government
- An online civil engineer database to offer its service

Expectations: He wants to offer its services to customers.

4.4.6 Technical Chamber of Greece (TEE)

Role

It is a professional body that represents and syndicates engineers. The TEE provides a database to look for a civil engineer.

Services offered:

- An online database, listing the available civil engineers, which are creditable to offer their services, as they are attributed to d by the law.

Services consumed:

None

Expectations: A user should be able to select a trusted civil engineer with appropriate qualifications.

4.4.7 Greek Government

Role

The Government sets the legislative framework, upon which the building process is based.

Services offered:

- A service to inform about law updates

Services consumed:

None

Expectations: The Greek citizens should be informed about law updates.

4.4.8 Real estate agent (REA)

Role

It is a company that holds a database of lots available for sale. It provides its services for a certain fee. The real estate agent offers its service in an online database. This may include the presentation of available lots in an online market place or the promotion of its service. This service includes the information about available lots which fit the requirements of a certain interested party. During the search for a suitable lot, he is the link between the interested party and the lot owners and organizes guided tours to the selected lots.

Services offered:

- Information about available lots and its specifications

Services consumed:

- Online database to promote its service.
- Internet based information services

Expectations: He wants to sell a maximal number of lots.

4.4.9 Bank (loan creditor of the interested party)

Role

If the interested party is asking for a credit of a certain bank, this bank requires information about the purchase object and the potential beneficiary.

Services offered:

- Credit

Services consumed:

- Value estimation of the lot
- Identity check
- Credit rating

Expectations: The bank wants credit receivers which are able to pay their debts.

4.4.10 Fora/citizen communities

Role

Any fora or citizen communities related to acquiring land, managing land and issuing a building permit. They may be considered as providers of information additional or supportive to interested party’s decision making process

Services offered:

- RSS-based information updates

Services consumed:

None

Expectations: To support the decision making process

4.5 User stories description

The property management and e-governance scenario can be realised through the following user stories.

User story C1 - Searching for the lot	
Description	This user story covers represents the situation, in which an interested stakeholder wishes to find an available lot in a specific geographical area within the limits of the Municipality of Athens. The story assumes that an application developer has implemented the DoUP application for the interested stakeholders to access all the necessary information when searching for a lot. The application scenario includes the following phases: • Publishing the lot information on the Web

	• Submitting a query for available lots searching Retrieving the available lots satisfying the query request • Requesting for additional information with respect to the desired lot(s) Through this application, lot owners or real estate agents may provide information about the lots they intend to make available for sale. The respective information can be spread to different providers through a simple click, as the application is delegated with the task to distribute the lot publication information to selected applications provided either by the Municipality of Athens or any other third party Real Estate application. In order to do so, the lot owners and the real estate agents should be granted secure access to the DoUP application in order to verify that the information provided by the lot owner is creditable and can be published. An Interested Party looks for available lots in a specific geographical area of the Municipality of Athens. He can thus access the DoUP application and identify his needs to formulate the query. At the background, the application analyses the query request and invokes a service, which redirects the query to the available lot information providers. The query returns back to the Interested Party a map with the available lots. When the map user clicks on a certain lot, the DoUP application projects the lot specific information by exploiting a composite service that aggregates the data found in the repositories of the third party Real Estate applications and the Municipality of Athens one. This data may include the following: • The map of the lot surrounding area, which is already provided by a dedicated service from the Municipality of Athens • The lot building terms and other government-related information about the selected lots (i.e. laws and regulations etc.), which are aggregated as part of the services provided by the DoUP and report on the building restrictions and other terms that apply to the specific lot. Apart from collecting all the regulations and procedure information, the Interested Party can go one step further and investigate on any background information, which is available through i.e. fora/citizen communities commenting on the quality of the urban area around the lot of interest, any costs related etc. Such user comments can be provided through services, which aggregate the discussing issues from fora or other governmental sources, and can be deemed as important to positively influence the Interested Parties' experience and affect their final decision on the lot selection.
Involved roles	Interested Party, DoUP-Municipality of Athens, Lot owner, Real Estate Agent, Greek Government, Solicitor, Fora/Citizen communities
Outcome	The Interested Party has made use of the DoUP application to locate the most appropriate lot.

Table 9: Case study C: User story C1

User story C2–Managing the lot	
Description	This user story refers to the situation, in which an Interested Party has identified the appropriate lot and wishes to proceed with acquiring it. In order to do so, he may access the DoUP application to request for a bank loan, subject to suitable offerings and conditions. The application connects to an available bank or financial institutions database or application to forward the loan request. The request to the bank includes as much information as possible so that the credit score is affordable and precise and the bank can make more accurate decisions when evaluating chances for or against the loan (and probably tailor a better price for the interested party). The bank representative can subsequently process the loan application by bringing together the necessary qualitative and quantitative data resulting from various information sources. The dedicated banking application integrates all the available data by invoking the appropriate services. It becomes apparent that talking about a scenario that could involve financial transactions in terms of loan requesting, these services should be secured and trusted, so as the provided information to be as accurate as possible. Through the effective processing of such data, the bank representative can eventually invoke the credit scoring computation algorithm and notify the Interested Party on the outcome of the loan request.
Involved roles	Interested Party, DoUp, Bank, Solicitor
Outcome	The Interested Party has made use of the DoUP application to effectively manage the lot property.

Table 10: Case study C: User story C2

User story C3 –Issuing the house building permit	
Description	This user story refers to the last part of the scenario for searching a lot and issuing a house building permit. The story begins with the selection of a Civil Engineer, who will be responsible for governing the principal steps and the procedure flows needed, in order to interact with the public authorities, and gather all the information required for submitting the building permit application form. In that respect, the Interested Party enters the DoUP application and requests for the creditable list of Civil Engineers from the Technical Chamber of Greece (TCG). The composite service on the background, along with the detailed list, retrieves the engineers' related information, such as availability and pricing, as well as recommendations and rating from different discussion fora. After assigning the issuing of the house building permit to a specific Civil Engineer, the latter acts on behalf of the Interested Party and accesses the DoUP application to first get informed on legislative framework applied to the selected lot and then gather all the necessary documentation to submit the house building permit application request form. Only the absolutely necessary data is requested in the form, which is

	communicated to the DoUP clerk for validation. The same application can be subsequently used from the clerk to gather all the appropriate supportive documents to proceed with the issuing of the permit. Since such documents may come from various other governmental bodies, the application exploits a composite service to collect the distributed information into a convenient to the clerk form. At regular intervals, the Civil Engineer invokes the associated services to monitor the status of the application request for issuing the house building permit, through the notification service, which is exposed by the DoUP system. Finally, this story can be extended to comply with the practices in other countries, such as in Germany, in which a solicitor is delegated with all the legal issues on behalf of the interested party, along with the Civil Engineer.
Involved roles	Interested Party, TEE (TCG) Registry, Civil Engineer, DoUP, Solicitor
Outcome	The Interested Party has issued the house building permit and can proceed with the construction of the house.

Table 11: Case study C: User story C3

4.6 Domain constraints

This section deals with the features of the land acquiring domain that could limit the design and development of the case study.

These features are mainly related to:

- Regulation Framework
- Reluctance to use the services.
- Single sign-on potential (SSO)

One of the main constraints when dealing with the land acquiring domain is the restriction imposed from the legislative framework. This framework can change between areas (e.g. countries) or periods of time. Most of the times these changes are not affecting the architecture of the solution but in some cases whole parts should be dropped off or redesigned. As a result the parts of the case study should be as loosely connected as possible in order to avoid the need of cascading changes.

The concept of e-governance is new to some countries, such as Greece. As a result many citizens/interested stakeholders will be unwilling to initially trust the services. This will be more apparent on services that initiate transactions with public services, such as the issuance of a building permit. A lot of time should be allowed before these services reach their full potential. A similar problem will arise with the cooperation of Real Estate Agents. These agents will be reluctant to share their estate databases, because they fear of being bypassed. Thus, measures should be taken to make the REAs more willing to co-operate.

The use of a SSO service would greatly enhance the usability of the solution. However many service providers, especially the ones belonging to the public sector, will need strong assurances of the end user’s identity. The provider of the SSO service should also be one with strong enough trustworthiness to be accepted by both service providers as well as end users.

4.7 Domain specific requirements

In this section requirements related to the land-buying through government services are collected.

4.7.1 Security requirements

Requirement ID – Type:	6C.1 – F
Requirement Name:	Provide authenticated access to services
Description:	Implement authentication mechanisms for accessing the services and resources foreseen for this case study
Rationale:	All the roles participating should have access to the provided services and resources through a secure way. Depending on the data exchanged and the security critically, the authentication mechanism might be different.

Requirement ID – Type:	6C.2– F
Requirement Name:	Provide single sign on
Description:	Accessing services offered by different Service Providers is enabled through a single point for submitting the user credentials
Rationale:	Services are offered by multiple providers. Secure access to such resources should be effective through a single sign on process, which prevents users from maintaining multiple relations with different service providers and submitting various credentials for accessing these resources

Requirement ID – Type:	6C.3– F
Requirement Name:	Publish service trust level
Description:	The service trust level should be made available by the relevant service owner, who can also specify the trust properties for accessing the specific service resources
Rationale:	In an e-government scenario, with multiple services being offered by different Service Providers, the publication of the services trust level is crucial in order to determine which of them can be exploited to access specific applications and resources. However, publishing service trust levels should be effective only through the authorised service authorities.

Requirement ID – Type:	6C.4– F
Requirement Name:	Trust relationship between roles
Description:	Establish mutual trustworthiness between roles exchanging critical data through services
Rationale:	In an e-government scenario, vast of data is exchanged, which can be classified under different categories, based on the data criticality. The mutual approval of the trustworthiness of the involved parties (service providers and their services, service consumers) should be established

Requirement ID – Type:	6C.5 – F
Requirement Name:	Enable policy-based access to services
Description:	Certain security policies are applied to govern the way that services are accessed by specific roles involved in the scenario
Rationale:	Business rules govern the transactions in an e-government scenario, especially with respect to interoperability patterns. Such rules are dominated from the relevant strategic and political decisions, which imply for specific security policies, when translating business interactions to system integration

Requirement ID – Type:	6C.6 – F
Requirement Name:	Enable policy-based composition of services
Description:	Services should be composed according to business-level interaction needs
Rationale:	Further to policy-based access to electronic services, particular political and strategic rules are applied to govern the way that services are composed and offered to the end users/stakeholders of the e-government scenario.

Requirement ID – Type:	6C.7 – F
Requirement Name:	Secure service design
Description:	Services should be modelled in a way that business level security concerns are effectively expressed
Rationale:	Security assertions, like trust and role-based access to services should be expressed in details when designing the relevant e-government services. The appropriate service modelling tool should be available to do so.

Requirement ID – Type:	6C.8– F
Requirement Name:	Secure data exchange
Description:	End users should be assured that their critical data will be securely exchanged
Rationale:	Data integrity is a crucial factor when delivering information in an e-government scenario

Requirement ID – Type:	6C.9– F
Requirement Name:	Service status monitoring at runtime
Description:	Monitor of the trust and security level of the service
Rationale:	Allow the service design may consider for effectively addressing the underlying security policies and trust levels, a mechanism is necessary to monitor whether the service status and security level is maintained at runtime

Requirement ID – Type:	6C.10– F
Requirement Name:	Maintain the security level of provided service compositions
Description:	Support for service replacement in case of trust level violation
Rationale:	Critical e-government infrastructures should take care for constantly monitoring the trust levels of service compositions

Requirement ID – Type:	6C.11 – F
Requirement Name:	Notification on service violation
Description:	Support the detection of changes in threat level and security requirements
Rationale:	The Aniketos platform should enable critical e-government infrastructures to identify the security gaps in the trust levels of service compositions

4.7.2 Technological requirements

Requirement ID – Type:	6C.12 – F
Requirement Name:	Provide secure Web-based access to public services
Description:	A Web 2.0 approach should be followed in order for the stakeholders involved in this case study to securely exchange information and complete their transactions.
Rationale:	According to the European Government Interoperability framework and the instantiation of it to each country, all the public services should be provided over the internet in a web-based access approach, enabling G2G, G2B and G2C interactions for accomplishing electronic public services. Such access should be secure and expose fundamental security attributes for the mutual realisation of security between the involved stakeholders.

Requirement ID – Type:	6C.13 – Q
Requirement Name:	Provide the applications extensibility to future functionalities
Description:	The implemented pilot should take care for the extensibility of interfaces and the appropriate extensions to future functionalities and compliance to modified business processes of the relevant government bodies
Rationale:	A SOA-based approach is necessary to fulfil the requirement of secure open interfaces by also exploiting open standards which enable the interface with other applications and integrate the interoperability scenario, which is dominant in modern e-Government Environments

4.7.3 Run-time requirements

Requirement ID – Type:	6C.14 – F
Requirement Name:	Context-aware service composition
Description:	Services could be recomposed based on contextual information (i.e. lot location is critical to determine building terms)
Rationale:	In order to target to personalised services, which is a general policy promoted by the relevant European initiatives in the e-Government domain, service composition could be enhanced through the exploitation of the available contextual information

Requirement ID – Type:	6C.15 – F
Requirement Name:	Offer service composition
Description:	Integrate content and services in a multi-owner environment by providing composition services based on application needs, while maintaining the appropriate functionality for the effective response to adjustments based on service status
Rationale:	Complex services are involved in the e-government service provision scenarios integrating data of different security level being offered from many providers. On top of that, the personalised of e-government services arises as the new trend in this domain. Service composition should enable the appropriate constitution service parts, which adapt to business needs and provide personalised access to public services

Requirement ID – Type:	6C.16 – F
Requirement Name:	Provide end user notification on service status
Description:	While service execution of a service composition, the users should be made aware of the service execution status, especially on the level to which the execution might have failed.
Rationale:	While a service composition has failed, users experience delay or service disruption, which is a black box for them, when trying to realise the problem. In such cases, the application should retrieve the event failure and interpret it to a meaningful message for them.

4.8 Storyboard

The storyboard lists the exact sequence of actions carried out by the users involved in the case study. It represents what will be shown with the realization of the case study.

In line with the user stories description in Section 4.5, this section develops a storyboard for depicting and realising the use case activities for the respective stories. A storyboard as such analyses all the activities performed and highlights the interaction of the end users with the system.

An overall structure of the case study C for the "Property management and e-governance scenario", including all the actors involved and the use cases to be accomplished is illustrated by Figure 21 as follows:

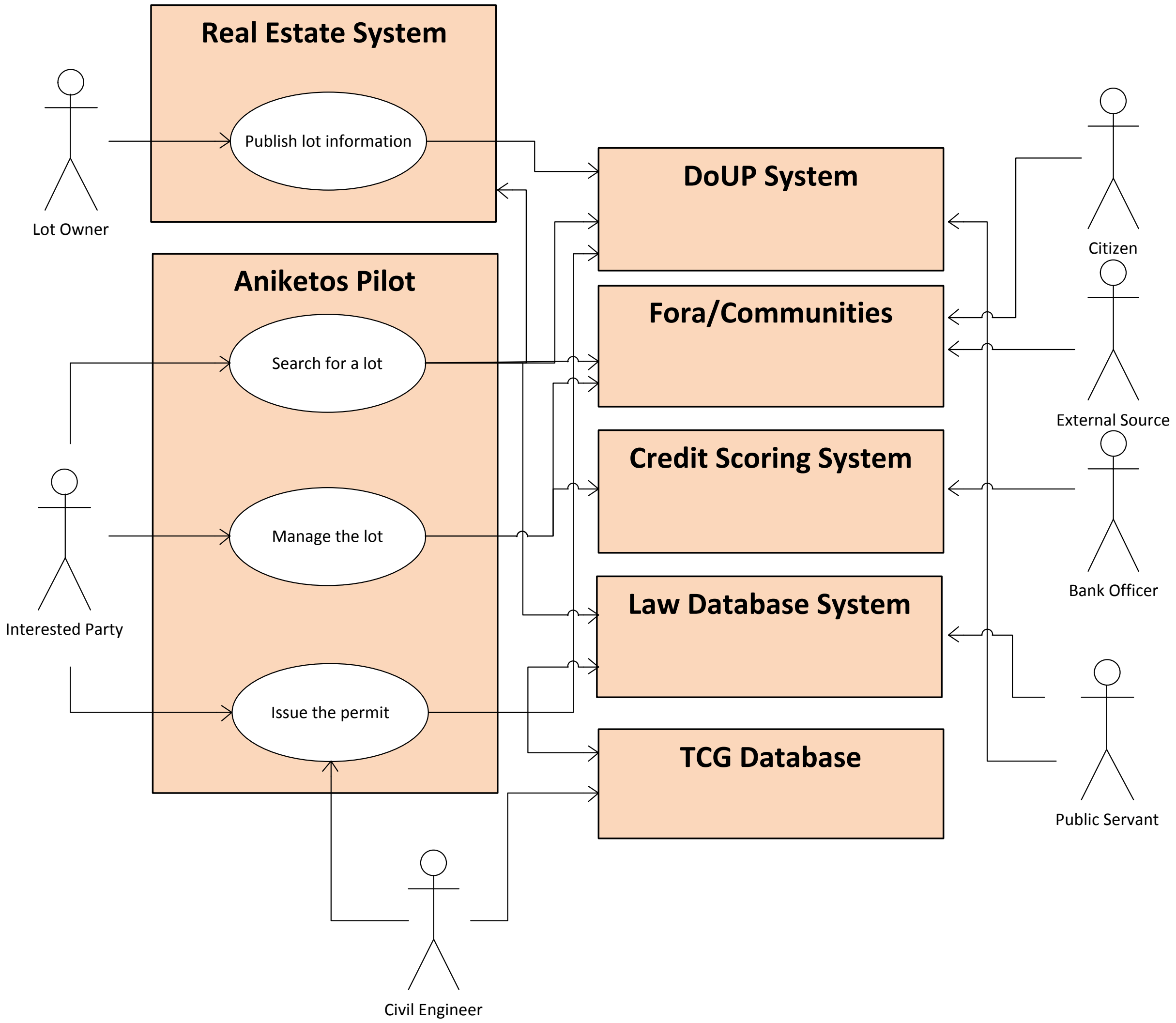


Figure 21: Realisation of the Case Study C

The storyboard is evolved through the following steps:

12. **Lot Owner provides lot information**

Lot owners provide information about lots they want to make available for sale. This information is uploaded to a database owned by the Municipality of Athens or to a 3rd party.

13. **Interested Party reviews an area**

Interested Party looks information on an area using map information provided by the Municipality of Athens

14. **Interested Party searches for lot**

Interested Party tries to locate an available lot. They use a composite service that aggregates the information found in 3rd party Real Estate's Databases as well as a database owned by the Municipality of Athens.

15. Interested Party gets information about a lot

Interested Party gathers information about a specific lot. To do so the interested party uses a composite service that provides:

- Maps of the lot's surrounding area. This service is provided by the Municipality of Athens and serves images containing the proper map.
- Building Terms. This service is provided by the Department of Urban Planning and reports the building restrictions and other terms that apply to the specific lot.
- User Comments. This service may be provided by one or more Fora and aggregates comments concerning the specific lot, or the area it is located in.

16. Interested Party looks for a creditor

Interested party looks for a bank offering suitable conditions for a credit. This search can be supported by 3rd party database.

17. Check of the credit rating

Interested party applies for a credit by the bank. The bank requires the following composites services using the ANIKETOS platform to check the credit rating of the interested party as well as the value of the lot. The composite service for the credit rating of the interested party includes

- The bank checks the identity of the interested party. This can be provided by an identity card (handed in personally) or the opening of a salary account with a certain monthly income hosted by this bank. Voluntarily, this can also be modelled as a service allowing the legitimisation (authentication) using an e-identity card (e.g., the recently issued ID card in Germany that support means for the strong authentication over the Internet).
- The bank checks the income of the interested party.
- The bank demands further services of scoring agencies to check the credit rating of the interested party (e.g. SCHUFA, for more information see http://www.schufa.de/de/home/)

The composite service for estimation of the appraisal value contains the following services

- The bank demands information about information about the lot: the information about the size, the site, and land charges are electronically provided by the “Grundbuchamt” in Germany.
- The bank will send an expert to evaluate this lot. Eventually, further information can be provided by commercial services.
- Based on this information, the bank is able to estimate the lot.

18. Grant the credit

Based on the information about the interested party and the lot, the bank can grant the credit.

19. Interested Party looks for an available Civil Engineer

Interested Party uses a service to search for a Civil Engineer Registry. He is provided with engineers’ related information such as availability and pricing.

20. Interested Party selects a Civil Engineer

Interested Party selects an engineer to acquire the building permit on behalf of him. A trust relationship between the IP and the engineer is established for the purpose of the permit's acquisition.

21. Civil Engineer Checks the Permit's Status

A civil engineer uses a service provided by the Department of Urban Planning to check the process status of the permit's acquisition.

22. Civil Engineer updates his data on the Civil Engineer Registry

A civil engineer uses a service to update his availability, pricing and other information on the Civil Engineer Registry.

23. Civil Engineer/Interested Party gets informed about the current legislative framework

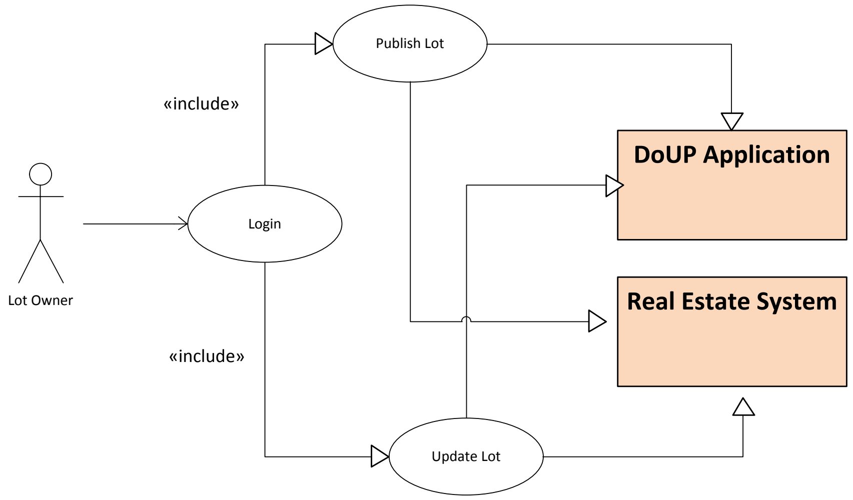
A civil engineer or an interested party can get information about current laws concerning the building process using a service provided by the Department of Urban Planning.

24. Department of Urban Planning updates information

Department of Urban Planning updates information about building terms/ legislative framework.

In order to better visualise the storyboard, the above mentioned steps are grouped by exploiting the user stories presented on Section 4.5. A structured form is used for this visualisation, which includes the triggering condition for each story, the potential input/interaction required from the users' side, the association with the activity steps and a use case diagram of the story.

4.8.1 Storyboard for C1

Purpose	Performing search to investigate on candidate lots for acquisition
Triggering Conditions	The user (Interested Party) specifies the criteria and preferences for identifying the appropriate lot.
Result	The user (Interested Party) gets all the information for the selected lot.
Activity Steps Involved	1. Lot Owner provides lot information 2. Interested Party reviews an area 3. Interested Party searches for lot 4. Interested Party gets information about a lot 5. The lot of interest is selected
Use Case Diagram	 Publish Lot «include» DoUP Application Login Lot Owner Real Estate System «include» Update Lot

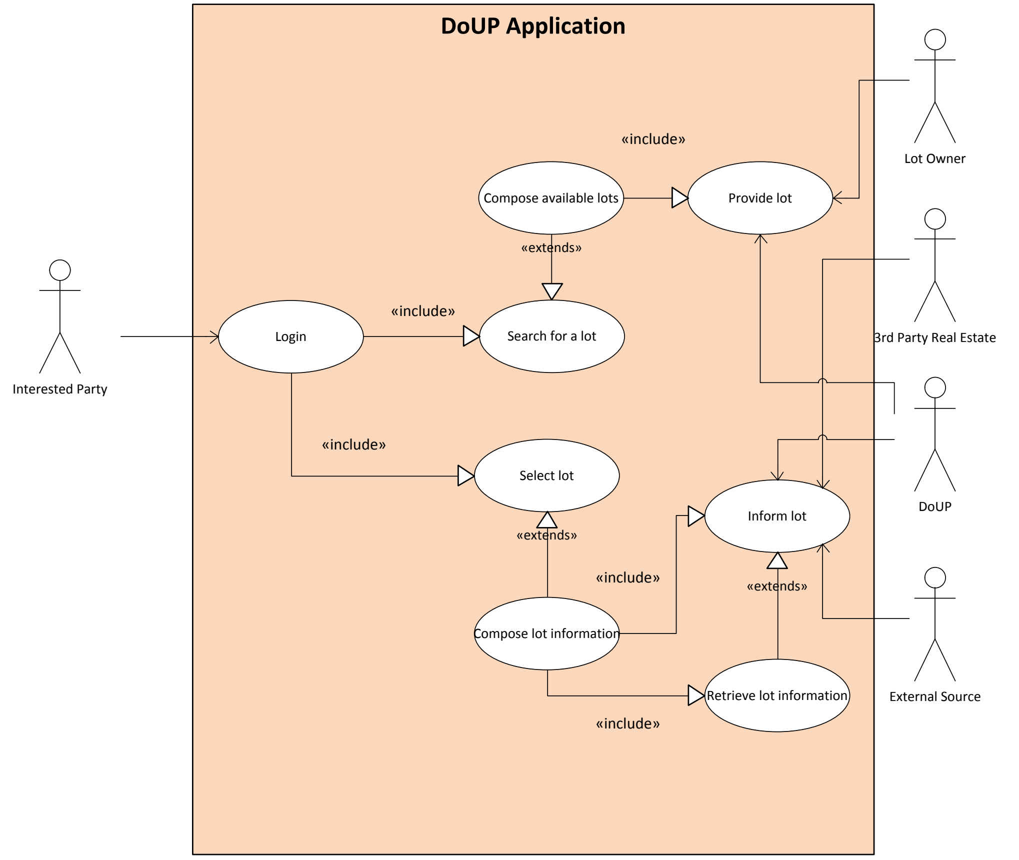
	

Table 12: Storyboard for C1

4.8.2 Storyboard for C2

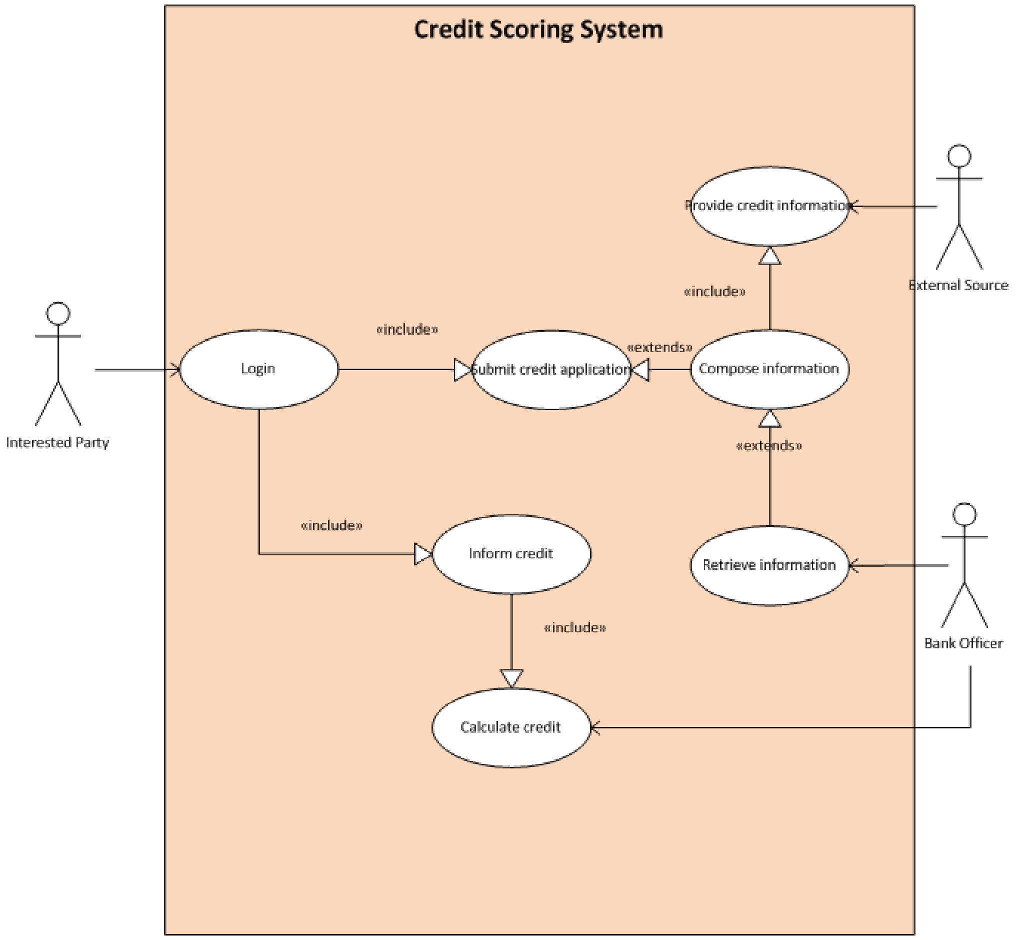
Purpose	Taking the appropriate actions to acquire the lot
Triggering Conditions	The user (Interested Party) identifies the method to acquire the selected lot
Result	The user (Interested Party) acquires the lot
Activity Steps Involved	1. Interested Party looks for a creditor 2. Check of the credit rating 3. Grant the credit
Use Case Diagram	 Credit Scoring System Provide credit information External Source «include» Interested Party Login «include» Submit credit application «extends» Compose information «extends» «include» Inform credit Retrieve information Bank Officer «include» Calculate credit

Table 13: Storyboard for C2

4.8.3 Storyboard for C3

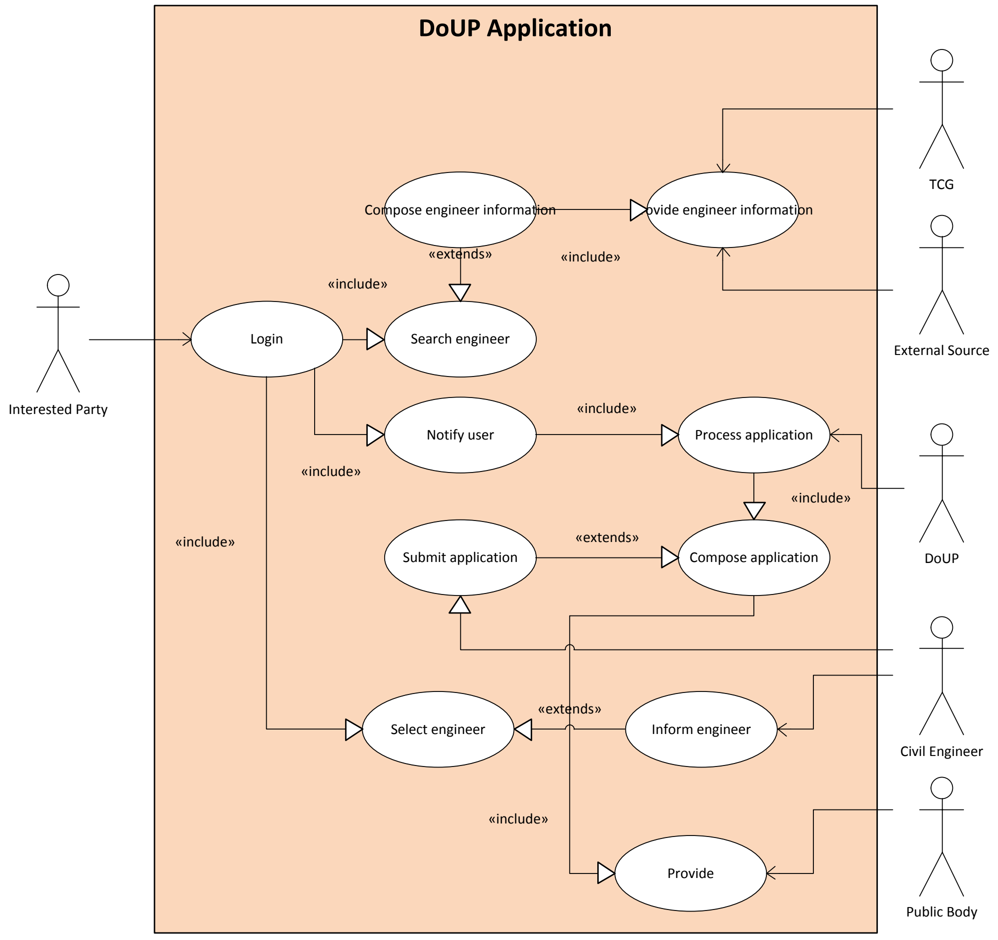
Purpose	Making the application for issuing the house building permit
Triggering Conditions	The user (Interested Party)delegates an authorised engineer to issue the house building permit
Result	The user (Interested Party) is allowed to start building on the lot
Activity Steps Involved	1. Interested Party looks for an available Civil Engineer 2. Interested Party selects a Civil Engineer 3. Civil Engineer Checks the Permit's Status 4. Civil Engineer updates his data on the Civil Engineer Registry 5. Civil Engineer gets informed about the current legislative framework 6. Department of Urban Planning updates information
Use Case Diagram	 DoUP Application TCG External Source Interested Party DoUP Civil Engineer Public Body Compose engineer information ovide engineer information «extends» «include» «include» Login Search engineer Notify user «include» Process application «include» «include» «include» Submit application «extends» Compose application Select engineer «extends» Inform engineer «include» Provide

Table 14: Storyboard for C3

5 Conclusion/Further work

The analysis of the industrial case studies provided in this deliverable has the aim to define well-suited contexts to prove Aniketos technologies and functionalities. Three application domains, namely telecommunication, ATM and e-Government, have been selected as representatives of areas in which the development of enhanced future composite services is envisaged.

Before dealing with further work needed to realise the industrial case studies, let’s resume briefly the objectives and scopes identified for each case study.

Case Study A deals with the possibility for a telecom operator to exploit the Aniketos platform functionalities to move forward in its role so as to be a player in the Web 2.0 world, thus realizing the so-called Telco 2.0 business model. Thanks to the Aniketos design-time and runtime support the telecom operator is enabled to compose and to expose secure and trustworthy services. By differentiating its offerings, the telecom operator will be allowed to face competition with web service providers: the key is to provide to its customers personalized services, which entails the handling of end user personal data. In this context, the targeted end user is the common user that browses the web in order to access services provided by multiple service providers; so, a key point is to make user experience simplified and most of all to assure the protection of personal data. Thus, Case Study A deals with the privacy issues that can arise and gives a possible solution with the introduction of an Identity Management (IdM) system.

Case Study B is devoted to ensure a secure and trustworthy exchange of safety-critical information among all the Air Traffic Management (ATM) and aviation stakeholders after the introduction of the System Wide Information Management (SWIM). This community is accustomed to building safety-cases and addressing the availability and integrity criteria with respect to non-intentional hazards. With the introduction of SWIM (potentially giving access to the ATM network to untrustworthy actors), these availability and integrity criteria together with the new confidentiality criterion must now be addressed with respect to malevolent behaviour. The ATM case-study represents high variety and complexity due to the multi-user and composite service environment involving a large amount of legacy systems and dealing with numerous international, national and local regulations. In Aniketos, Case Study B will be devoted to the application and evaluation in a real industrial domain of the design-time solutions provided by the Aniketos platform.

Case Study C refers to a real life application targeting the e-Government domain. It involves multiple service providers and consumers, who interact with each other to enable accessing the most up-to-date procedures, information on relevant regulations and advice on associated costs, which affect decisions when acquiring land and issuing the respective building permit. Within the scope of this case study, a number of security and trustworthiness requirements have been identified, which mainly refer to the corresponding problems being faced today when dealing with the traditional practices in similar application fields. As the information which is exchanged between the relevant stakeholders can be classified according to privacy and trustworthiness levels, this case study heavily involves the Aniketos project aspects for supporting security and trust in service composition of modern service-based systems. Currently, the available solutions lack on providing the adequate level of trust for the semi-automatic execution of the involved processes, thus they are actually based on face-to-face transactions. The orientation of the selected e-Government case study, which is proposed to be solved through the use of the Aniketos developments, is fully aligned to the strategic agenda for Digital Europe and the i2010 initiative, which guide the activities in the area of public service delivery for the next years. The identified gaps between the existing solutions and the principal requirements of security and trustworthiness can be effectively addressed through this Aniketos-based case study.

User stories have been provided for each case study; their realization will show the practical application of the Aniketos results to real life situations. The user stories have been drawn so as to evaluate critical functionalities of Aniketos platform:

- composition based on security properties and trust;

- runtime recomposition;
- service discovery based on trust and security properties;
- composition of services made up of components provided by several service providers;
- end user notification related to the execution of the composition;
- improvement of the user experience in accessing services offered by multiple services providers.

The content of the document will guide the implementation of the platform and it will constitute the reference document for subsequent deliverables, namely D6.2, D6.3 and D6.4.

Specifically, in D6.2 a work plan for the execution of the case studies will be provided. The work plan has the aim to schedule the activities related to the design and implementation of the case studies. A set of periodic evaluations will be planned, whose results will be collected in D6.3 and D6.4. In particular D6.3 will collect the reports and recommendations resulting from the initial application to the case studies of Aniketos outcomes. The final outcomes resulting from the adoption of the Aniketos platform will be collected in D6.4.

References

[1] SWIM-SUIT Information Security Requirements (D1.4.1), Issue 02, 28-05-2008, http://www.swim-suit.aero/swimsuit/projdoc.php?action=download&id=56

[2] SWIM-SUIT - Overall SWIM users requirements (D1.5.2), Issue 01, 10-06-2010,

[3] EUROCAE Flight Object Interoperability Specification (ED-133), June 2009, http://boutique.eurocae.net/catalog/advanced_search_result.php?keywords=ed-133&x=0&y=0

[4] Celtic-Plus Purple Book – version 2011, http://www.celtic-initiative.org/PurpleBook+/Celtic-Plus%20Purple%20Book-2011-web.pdf

[5] ITU-T Y.2011 Next Generation Networks – Frameworks and functional architecture models.

[6] ITU-T Y.2720 NGN identity management framework.

[7] Maler, Eve and Drummond Reed, "The Venn of Identity: Options and Issues in Federated Identity Management," IEEE Security and Privacy, Vol. 6, No. 2, March/April 2008, pp. 16-23

Appendix A. Case study B

A.1 ATM: short domain glossary

This glossary aims to clarify some commonly used terms in the Air Traffic Management (ATM) domain jargon. When some of the terms defined below make use of other terms defined in this glossary, they can normally be reached through hypertext links. The terms are listed in alphabetical order. Note that this glossary poorly addresses the ATM stakeholder roles because §3.4 of this document is devoted exclusively to the definition of users.

DEF-001

Aerodrome Definition

An aerodrome is a defined area on land or water (including any buildings, installations, and equipment) intended to be used either wholly or in part for arrival, departure and surface movement of aircraft.

Note: the term "airport" is often inappropriately used instead of "aerodrome".

DEF-002

Aircraft Definition

An aircraft is any machine that can derive support in the atmosphere from the reaction of the air other than the reactions of the air against the surface of the earth3. Thus, the term aircraft refers to fixed wing and rotary wing (helicopters) powered aircraft, and balloons.

DEF-003

Air Traffic Control (Service) Definition

Air traffic control (ATC) is a service provided for the purpose of:

- preventing collisions:
  - between aircraft, and
  - on the manoeuvring area, between aircraft and obstructions; and
- expediting and maintaining an orderly flow of air traffic.

ATC services are normally provided by an air traffic control unit.

DEF-004

Air Traffic Control Unit Definition

Air traffic control units are specialised in providing air traffic control services, but they are also responsible for flight information service (FIS) and alerting service to pilots (i.e. assisting aircraft in difficulty and initiating search and rescue).

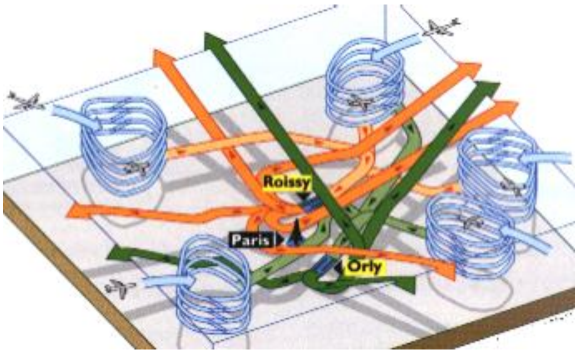
[3] This typically excludes hovercraft.

An air traffic control unit is typically responsible for:

- aerodrome control service, in which case it is called the aerodrome control tower (TWR);
- approach control service, in which case it is called the approach control unit (APP);
- area control service, in which case it is called the area control centre (ACC) or upper area control centre (UAC).

DEF-005

Air Traffic Flow Management Definition



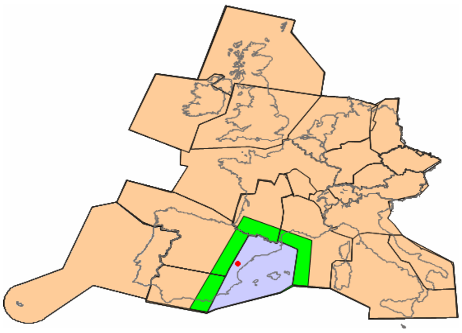
Air traffic flow management (ATFM) is a part and a function of the air traffic management (ATM) system. The objective of ATFM is to ensure an optimum flow of air traffic through areas in times when demand exceeds or is expected to exceed the available capacity of the air traffic control (ATC) system. ATFM assists ATC in achieving the most efficient utilisation of available airspace and aerodrome capacity while keeping delays and subsequent costs to a minimum.

The Central Flow Management Unit (CFMU) provides an ATFM service to airspace users throughout to European Civil Aviation Conference (ECAC) States.

DEF-006

Air Traffic Management Definition

The purpose of air traffic management (ATM) is to enable aircraft operators to meet their planned departure and arrival times. This includes helping aircraft adhere to optimal flight profiles, minimising constraints and ensuring safety. ATM relies on the availability of communication, navigation and surveillance (CNS) system to provide the information on individual aircraft position and intent to match the traffic with the available controller capacity.



ATM consists of a ground and air part, both needed to ensure the safe and efficient movement of aircraft during all phases of operation.

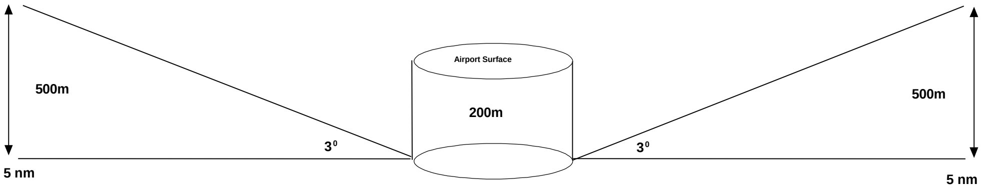
The International Civil Aviation Organisation (ICAO) defines ATM as:

- air space management (ASM),
- air traffic flow management (ATFM), and
- air traffic control (ATC),
- flight information service (FIS), which gives useful information and advise for the safe and efficient conduct of flights, such as the status of navaids, bad weather, closed airfields, etc.

DEF-007

Approach Area Definition

The approach area of a runway heading is defined as the area from the runway threshold out to a distance of 5 nautical miles and within the runway's glide path.



The approach area of an aerodrome, is the sum of the approach areas of all runway headings defined for that aerodrome.

DEF-008

Apron Definition

An apron is a defined area on an aerodrome intended to accommodate aircraft for purposes of loading or unloading passengers, mail or cargo, fuelling, parking or maintenance.

DEF-009

Manoeuvring Area Definition

The manoeuvring area is that part of an aerodrome to be used for takeoff, landing and taxiing of aircraft, excluding aprons.

DEF-010

Runway, Runway Heading and Runway Strip Definition

In a geographical context:

- the term runway strip refers to the landing / takeoff surface, whilst
- the term runway, used alone, refers to the runway strip plus those portions of the approach and departure paths used in common by all aircraft.

In an operational context, the terms runway heading or runway direction should be preferred. Runway headings at an aerodrome are designated according to their compass bearings rounded off to the nearest 10°, with the final zero omitted. A single runway usually corresponds to two runway headings, covering the same physical area. Where two parallel runway headings are available, they are known as left and right respectively.