Selected Change Requirements and Security Properties

A. Armenteros (TID), B. Chetali (GTO), M. Felici (DBL), F. Massacci (UNITN), V. Meduri (DBL), A. Tedeschi (DBL),

Document information

Document Number	D1.1.1
Document Title	Selected Change Requirements and Security Properties
Version	3.0
Status	Final
Work Package	WP 1
Deliverable Type	Report
Contractual Date of Delivery	18/06/2010
Actual Date of Delivery	18/06/2010
Responsible Unit	WP1
Contributors	DBL,GTO, TID, UNITN
Keyword List	

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	16/04/2010	Draft	B. Chetali (GTO)	Initial draft
0.2	17/04/2010	Draft	M. Felici, V. Meduri, A. Tedeschi (DBL)	Main changes and additions to: Executive Summary, ATM change requirements and security properties, and HOMES change requirements and security properties
0.4	19/04/2010	Draft	M. Felici, V. Meduri, A. Tedeschi (DBL)	ATM Change Requirements updated
0.6	22/04/2010	Draft	M. Felici, V. Meduri, A. Tedeschi (DBL)	Suggestion by WP1 partners integrated
1.1	03/06/2010	Draft	M. Felici, V. Meduri, A. Tedeschi (DBL)	Revised ATM Changes requirements according to the comments and modifications agreed in the conf call of 28/05/2010; Information of the WPs coverage w.r.t. the case studies
1.3	07/06/2010	Draft	B.Chetali	Update according to the conf call
1.4	08/06/2010	Draft	M. Felici, V. Meduri, A. Tedeschi (DBL)	Updates on the ATM Case Study
1.6	11/06/2010	Draft	A. Tedeshi (DBL), A. Armenteros Paheco (TID)	Updates on the TID Case Study
1.7	11/06/2010	Draft	B.Chetali	Updates according to the conf call

1.8	14/06/2010	Draft	M. Felici, V. Meduri, A. Tedeschi (DBL)	Minor changes to the ATM case study, and new WPs and Case Studies interaction description according to the conference call on 11/6/2010
2.0	16/06/2010	Draft	A. Armenteros Pacheco (TID), A. Tedeschi (DBL)	HOMES Case Study updated
2.1	17/06/2010	Draft	E. Chiarani (UNITN)	Formal quality check
2.2	17/06/2010	Draft	B.Chetali (GTO)	Minor mistakes in POPS
3.0	18/06/2010	Final	F. Massacci (UNITN)	Final Revision

Executive summary

This document identifies selected change requirements and security properties drawn from the three case studies in WP1: HOMES (led by TID), POPS (led by GTO) and ATM (led by DBL). The selected requirements and properties narrow the scope of analysis and applicability for the SecureChange artefacts. They have been drawn from *D1.1 – Description of Scenarios and Their Requirements*. They enable us to identify change requirements clearly, and those security properties that are critical and relevant for the applicability and effectiveness of SecureChange artefacts.

Table of Contents

DOCUMENT INFORMATION 1

DOCUMENT CHANGE RECORD 2

EXECUTIVE SUMMARY 4

TABLE OF CONTENTS 5

1 INTRODUCTION 6

2 ATM CASE STUDY 7

2.1 Change Requirements 7
2.1.1 Process Level Change 7
2.1.2 Organizational Level Change 7

2.2 Security Properties 8

3 HOME CASE STUDY 9

3.1 Change Requirements 9
3.1.1 Core Security Module Update 9
3.1.2 Bundle Lifecycle operations 9

3.2 Security Properties 9

4 POPS CASE STUDY 11

4.1 Change Requirements 11
4.1.1 Specification evolution 11
4.1.2 Software update 11

4.2 Security properties 11

5 CASE STUDIES' COVERAGE 13

6 GLOSSARY 15

1 Introduction

This document presents the properties drawn from each case study that will be used as a “fil directeur” for all the work packages. The three case studies lie on different complementary domains, in the aim of showing the SecureChange approach in the widest range possible. They are representative of relevant but not exclusive application domains of SecureChange output. The case studies, named according to their domains, are these ones:

- Air Traffic Management case study (ATM)
- Home Network case study (HOMES)
- Smart Card case study (POPS)

Each case study comes with his specificities of change and impact. Therefore the analysis of the applicability of developed technologies will follow different feasibility and evaluation criteria. In particular, the requirements changes characterising the three case studies fall into three different types: ***Changes in Process***, ***Changes in Configuration***, and ***Changes in Software***.

The ATM case study involves various change requirements due to the introduction of new tools. The ATM case study is concerned with how such new tools affect organisational as well as operational aspects. The ATM case study is characterised by ***Changes in Process***.

The HOMES case study is focused on change requirements on policies and critical on software modules providing critical security features. HOMES deals mainly with **Changes in Configuration.**

The POPS case study focuses on an UICC card made of integrated circuit (hardware) and an operating system base on JavaCard and GlobalPlatform specification. This object has been security certified before it issuing, but his life-cycle includes change that could be done in the field. These changes result from adding of a new application while preserving the implemented security. Therefore POPS case study is mainly concerned with **changes in Software**.

2 ATM Case Study

The ATM case study is concerned with **changes in the operational processes of managing air traffic in Terminal Areas**. Arrival management is a very complex process, involving different actors. Airport actors are private organizations and public authorities with different roles, responsibilities and needs. The subsequent introduction of new tools, i.e., the Queue Managers, and the introduction of a new ATM network for the sharing and management of information, affects the ATM system as a whole at a **process** and **organizational** level. The next section describes the selected requirements drawn from deliverable D1.1 **Errore. L'origine riferimento non è stata trovata.**.

2.1 Change Requirements

2.1.1 Process Level Change

ATM procedures need to be updated in order to accommodate the introduction of the AMAN (**A**rrival **MAN**ager). The AMAN is an aircraft arrival sequencing tool helping to manage and better organise the air traffic flow in the approach phase. It is directly linked to the airport organisation and the turnaround process, because arrival sequencing/metering is important for airline operational control and airport operations (e.g., ground handlers, catering services, airlines, security and health authorities, etc.) in order to organise the ground services efficiently.

The introduction of the AMAN requires new operational procedures and functions (as described in the deliverable D1.1 **Errore. L'origine riferimento non è stata trovata.**). Such new procedures and functions are supported by a new information management system for the whole ATM, an IP based data transport network that will replace the current point to point communication systems with a ground/ground data sharing network which connects all the principal actors involved in the Airports Management and the Area Control Centers.

Goal: The resulting ATM system (with the AMAN and the communication network introduction) needs to comply with suitable security properties, which prevent from corruption, accidental or intentional loss of data and guarantee the integrity and confidentiality of the aircraft sensible data against malicious attacks or intrusions.

2.1.2 Organizational Level Change

The introduction of the AMAN affects Controller Working Positions (CWPs) as well as the Area Control Center (ACC) environment as a whole. The main foreseen changes (as described in the deliverable D1.1 **Errore. L'origine riferimento non è stata trovata.**) in the ACC from an operational and organizational point of view are the automation of tasks (i.e. the usage of the AMAN for the computation of the Arrival Sequence) that in advance were carried out by Air Traffic Controllers (ATCOs), a major involvement of the ATCOs of the upstream Sectors in the management of the inbound traffic.

These changes will also require the redefinition of the Coordinator of the Arrival Sequence Role, who will be responsible for monitoring and modifying the sequences generated by the AMAN, and providing information and updates to the Sectors.

Goal: The AMAN's interfaces that provide access to different roles and authorizations need to make information available only to authorized personnel or trusted systems.

2.2 Security Properties

The following security properties need to be guaranteed at the process and organizational level and will be the focus of the technical WPs.

Information Access. Authorized actors (or systems) must have access to confidential information regarding queue management in the terminal area. Access to information needs to comply with specific role-based access control rules drawn from the operational requirements.
Information Protection. Unauthorized actors (or systems) are not allowed to access confidential queue management information.
Information Provision. The provisioning of information regarding queue management sensitive data by specific actors (or systems) must be guaranteed 24 hours a day, 7 days a week, taking into account the kind of data shared, their confidentiality level and the different actors involved.
Information Need. Confidential queue management information can be accessed by authorized actors (or systems) only when the information is necessary for operational purposes, which may vary even in real time, due to particular conditions (bad weather, emergency status, etc.)

3 HOME Case Study

HOMES is focused on digital home networks where some sensible changes take place from the point of view of the security. We consider some changes, from the large set of changes that anyone may identify in this context, very related to configuration and deployment. Our target is the home gateway as a critical point in the home network.

3.1 Change Requirements

3.1.1 Core Security Module Update

Home Gateway has some security modules implementing NAC functional components like the PEP. NAC technology and its functional elements are properly described in the deliverable D1.1.. During the lifecycle of the whole system some component updates shall be required for various reasons (better performance, bug fixes, etc.). Updating one of these core security modules in the home gateway is a critical operation and a relevant change. Any attack or failure in this process may result extremely harmful.
A possible update on the core security modules could be the extension of information for the security assessment (more information in deliverable D1.1). In this case, the home gateway needs to be updated so that the new security status information is understood and assessed correctly.

Goal: Show that the security properties detailed below are still preserved after an update of a security module.

3.1.2 Bundle Lifecycle operations

A Home Gateway is also a service platform for the home. Customers can install new home services, upgrade or delete existing ones. This type of change is similar to the previous one but here services do not usually implement security functionality. The bundles installed on the home gateway are used for higher level applications. The services may come from third parties and therefore some similar control over this software must exist. Trust relationships among the customer, the service provider, and the third parties may evolve over time. However in some cases security bundles could deployed (provided by the operator)

Goal: Bundles have to be managed (update, addition, removal) in compliance with the trust relationships and assuring system consistency, i.e. the security properties need to be preserved despite these changes.

3.2 Security Properties

The following properties will be the focus of the technical WPs.

Secure extensibility. The home gateway can be extended at run time with additional general software (e.g. bundles) coming from third parties in many cases. Such extensions should be verified to be secure in the sense that they do not introduce unauthorized information leaks or the possibility of denial of service

Policy enforcement. The Policy Decision Point (PDP) is located in the security domain of the operator. The Policy Enforcement Point (PEP) is a core security module installed on the home gateway. The PEP always enforces policy decisions forwarded by the PDP so that only allowed actions can be carried out.

Resilience to trust changes. The system shall be able to accommodate a change in the trust relationships (among service provider, customers, 3rd parties) with a minimal impact on the software architecture

Security expandability. System security can be enhanced by taking advantage of the home gateway extension ability (mentioned in the Secure Extensibility property) through the deployment of new security services (e.g., deployment of a non-repudiation service bundle to ensure that neither service provider nor customer can later deny having sent/received a purchased service). The infrastructure shall be able to efficiently enforce such new requirements with a minimal impact on it.

4 POPS Case Study

An USIM card has been certified w.r.t. Common Criteria security certification V3.1. This means that the embedded software on this device ensures a set of properties related to (at least) **confidentiality** , i**ntegrity** and **availability** of its assets (but also non-repudiation, authentication, no by passability, etc).

But this “system” during its life cycle will evaluate. The Common Criteria impose that any change that occurs will lead to a re-certification of the card. As the evaluation process is expensive in term of cost and delay, we investigate means, that might be provided by the project, to speed up the re-certification of the card. The means are any kind of artefact that could be used for the evaluation: model, proof, test suites, etc

The objective is then to demonstrate this UICC card ensures those security properties after two realistic scenarios of changes, detailed below.

4.1 Change Requirements

4.1.1 Specification evolution

An UICC card embeds a component called the card manager, implemented according to GlobalPlatform specifications v2.1. This card component has been extensively verified and tested. The GlobalPlatform specification have been enhanced and extended and v2.2 has been issued. The card manager software component has been updated and extended against this new version. For simplicity reason, we restrict the 2.2 scope to the UICC configuration.

Goal: prove/demonstrate/test that the security properties are still preserved. For that we will concentrate on specific properties detailed below.

4.1.2 Software update

The certified UICC card is deployed in the field. The mobile operator, owner of the card, has a new partner, a bank. He loads a new security *domain (a Java Card application)* on the UICC (card) using an OTA mechanism. This bank will have the delegated management privilege from the Mobile Network Operator to manage its applications in a **confidential** way. In particular, the bank will use its security domain to load an e-purse on the card.

Goal: prove/demonstrate/test that the new application preserves (do not break) the consistency of the existing and implemented security policies. Again the specific properties are detailed below.

4.2 Security properties

The following properties will be the focus of the technical WPs.

Denial of service: Any application on the card do not generate a deny of service. This means that some robustness properties must be verified by the applets, such as no runtime exception, no infinite loop. Also the memory consumption must be bounded for the durability of the EEPROM and the Flash. For example, bounding the call-stack or detecting loop that updates the persistent memory.

Life-cycle consistency: Any command received by the card must respect the card and applet lifecycle. Its means that any command received in a state s leads to a state s' and the resulting transition from s to s' is correct w.r.t. the specifications.

Information protection: The applications on the card must be "isolated" (segregation), that means no illegal access to the data from one application to another. For that several security policies are described and assumed to be implemented on the card, like the JavaCard firewall (access control implemented by the virtual machine) or the security domains of GP. Therefore, some properties must be verified, when an applet is added on the card, like the consistency of the security domain hierarchy, the non-violation of the information flow policy implemented on the card, etc.

Secure communication: The secure Channel protocol provides a secure communication between a card and the off-card entity during an application session. It means that the protocol must ensure entity authentication, an entity is an off-card one as the issuer (terminal) or an on-card entity. Each entity proves its authenticity to the other entity. The protocol must ensures also integrity and confidentiality of the transmitted data.

5 Case Studies' Coverage

Table 1 shows the interactions among the technical WPs and the Case Studies.

Technical WP	Case Study
WP2	ATM, HOMES
WP3	ATM, POPS
WP4	ATM, POPS
WP5	ATM, HOMES
WP6	POPS, HOMES
WP7	POPS, HOMES

Table 1 Interactions among Technical WPs and Case Studies.

WP6 and WP7 will not to work on the ATM case study as all techniques developed in these work packages need executable code to be appled and this is not available in the ATM case study.

In particular for WP6 the development-time tasks (Task 6.1 and 6.2) need source code that can then be annotated to have it pass verification. The on-device tasks (Tasks 6.3, 6.4 and 6.5) require Java bytecode: they statically analyze bytecode during the loading process. CAlso for WP7, the project needs to have detailed functional behaviours to be able to produce a test model. Also for the validation of generated tests an implementation is needed to execute tests in order to validate the tools developed in T7.3 and provide feedbacks for D7.4.

Of course legacy software is used in the broad ATM domain but it would not be meaningful to test the techniques of the project on a software that will disappear in less than 5 years and will be possibly implemented using completely different languages.

In order to achieve few, streamlined, and orchestrated research strands, the technical integration among the WPs have been focussed and driven by the case studies. Figure 1 reports the main integration links in the project by means of relevant case study addressed by technical WPs. The meaning of a link is that a clear formal relation between the artifacts developed on the WPs on either side will be identified and the label define the case study on which such relation will be exemplified.

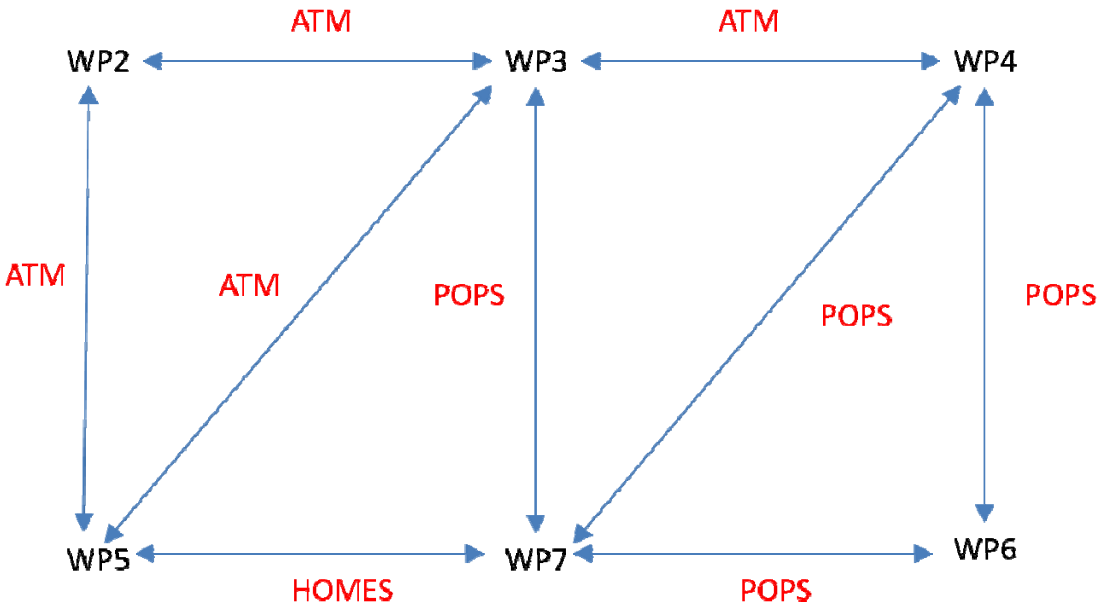

Figure 1 Main Case Studies that ensure the integration among technical WPs.

It is expected that further integration clusters will emerge from the work on shared case studies. For instance, an integration cluster is expected among WP2, WP3, WP4 and WP5 resulting from the collaborations on the ATM case study. Similarly, another integration cluster will emerge among WP3, WP4, WP6 and WP7. Emerging clusters resulting from the collaborations over selected changes requirements and security properties drawn from the shared case studies will strength the integration of the different WPs.

6 Glossary

Acronyms	Definition
ACC	Area Control Center
AID	Application identifier
AMAN	Arrival MANager
APDU	Application Protocol Data Unit
ATC	Air Traffic Control
ATCO	Air Traffic COntroller
ATM	Air Traffic Management
CWP	Controller Working Position
DHCP	Dynamic Host Client Protocol
DMAN	Departure MANager
EMV	Europa MasterCard Visa
FTTP	Fiber To The Premises
ISD	Issuer Security Domain
NAC	Network Access Control
NAT	Network Address Translation
OSGi	Open Service Gateway Initiative.
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PLC	Power Line Communication
PPPOE	Point-to-Point Protocol over Ethernet
QOS	Quality of Service
SCP	Secure Channel Protocol
SIM	Subscriber Identity Module
TMA	TerMinal Area
USIM	Universal Subscriber Identity Module
VPN	Virtual Private Network
WIMAX	Worldwide Interoperability for Microwave Access