



InspireD

D19 AOPOC Implementation Report

CONTRACT NO	INSPIRED IST-2003-507894
DATE	18/12/2006
ABSTRACT	Preface document for the individual AOPOC implementation reports
AUTHOR, COMPANY	Walter Hinz, G&D
WORKPACKAGE	WP2.2, WP2.3, WP2.4
CONFIDENTIALITY LEVEL	CO
FILING CODE	INSPIRED_D19_AOPOC0_R1.0

DOCUMENT HISTORY

<u>Release</u>	<u>Date</u>	<u>Reason of change</u>	<u>Status</u>	<u>Distribution</u>
R0.01	12.10.06	Initial document	draft	
R1.0	18.12.06	Final document for submission	final	ARTTIC and EC

Table of Contents

1.	INTRODUCTION	2
2.	LIST OF AOPOCS	2
2.1	AOPOC #1: AUTHENTICATION GATEWAY.....	3
2.2	AOPOC #2: MOBILE DRM (FAIR USE)	3
2.3	AOPOC #3: MOBILE DRM.....	3
2.4	AOPOC #4: SMART MMC SERVER	3
2.5	AOPOC #5: WEB SERVICES	3
2.6	AOPOC #6: SECURE BROADCAST (PAY TV)	4
2.7	AOPOC #7: ANONYMOUS SERVICES ACCESS.....	4
2.8	AOPOC #8: BIOMETRY	4

1. Introduction

This document is an introduction to several implementation reports for a total of eight Application-Oriented Proofs-of-Concept (AOPOCs) that have been prepared as proofs of concept for the TPD. All these documents together constitute the deliverable D19.

The implementation reports have been prepared individually by the partners concerned and have been collected by the author of this preface. The following naming convention has been applied:

- The document title is always like “D19: AOPOC#x <AOPOC title> Implementation Report” where “x” is a number defined in the AOPOC table in the main section of this document below and where <AOPOC title> is the name given to the AOPOC (found in the same table).
- The document filename is then encoded as “INSPIRED_D19_AOPOCx_Rn.nn” (with extension according to the word processor) where “x” is again the AOPOC number and “n.nn” signifies the document revision

A high level overview description of the AOPOCs is part of the TPD AOPOC Overview [D5.2]. Further earlier InspiredD documents are referenced in the individual documents.

2. List of AOPOCs

Within the individual AOPOC implementation reports the AOPOCs listed in the following table have been described. Each AOPOC has been implemented by a partnership of some of the partners participating in the InspiredD project. The leading partner for each AOPOC is marked in the table with bold type.

In choosing the AOPOCs two different approaches have been followed. Some of the AOPOCs strictly refer to specific use cases while others follow a more general approach of providing an application platform. These different approaches are marked in the last column of the table

AOPOC #	AOPOC Name	Partners	Approach
1	Authentication Gateway (SSO)	G&D / IFX	use case driven
2	Mobile DRM (Fair Use)	ORGK / ORGA / STM	use case driven
3	Mobile DRM	AXA / ATR	use case driven
4	Smart MMC Server	GEM / ATR	platform driven
5	Web Services	OCS / IFX	platform driven
6	Secure Broadcast (Pay TV)	NDS / GEM	use case driven
7	Anonymous Services Access (DAA)	OCS / FT	platform driven
8	Biometry	AXA / ATR / ATG	platform driven

Table 1: List of AOPOCs

2.1 AOPOC #1: Authentication Gateway

The Authentication Gateway AOPOC is a model for a TPD application which enables a user to connect to his or her favorite web sites without being forced to always remember his or her access credentials. He or she only has to activate his or her TPD once, and afterwards the TPD supplies username/password credentials automatically whenever the user enters a web site wherever a login process is required.

2.2 AOPOC #2: Mobile DRM (fair use)

This implementation report covers the **Application-oriented Proof of Concept (AOPOC)** for a new kind of **Mobile Digital Rights Management** applications (**MDRM**) based on **Open Mobile Alliance's** DRM standard (**OMA** DRM specification 2.0).

The key is to put the user with his **Trusted Personal Device (TPD)** in a position where he or she can consume protected digital content (i.e. video, audio, text files) in a reliable and easy way on different host devices in a mobile and networked environment. Additionally the user is empowered to transfer digital rights to other users having a TPD (**Fair use**).

This report is based on the overall concept of the TPD as a new platform for smart cards and related devices. Its innovative features based on the technical specifications will be highlighted in the context of three MDRM usage scenarios.

The considered TPD target platform is the **TPD-SIM profile**. The actual hardware platform employed in the AOPOC is supplied by ST-Microelectronics. The embedded system software (OS) is provided by Sagem-Orga, and the application software part is developed by Orga Systems.

2.3 AOPOC #3: Mobile DRM

In the context of Mobile DRM, the TPD manages and handles content rights according to the OMA DRM scheme. Whenever content is rendered, the mobile handset retrieves the content keys from the TPD that acts as a proxy for the right issuer.

2.4 AOPOC #4: Smart MMC Server

The Smart MMC Server proof of concept consists in a platform integrating innovative features such as Http Web Server, High Speed Protocol such as MMC, TCP/IP protocol and Mass Storage support. Through dedicated demos, Smart MMC Server Apoc is illustrating each of these innovative features.

2.5 AOPOC #5: Web Services

A TPD running a Web server embedded in a USB dongle. Here, the TPD acts as an innovative platform to enable the execution of Web Service based applications. An e-employment Web Service permits the automatic and secure matching of job offers and demands according to the holder's criteria with full respect of privacy.

2.6 AOPOC #6: Secure Broadcast (Pay TV)

Secure Broadcast, a TPD that functions as a secure token, allowing a secure encrypted broadcast to be received by a mobile device. The TPD, which is attached to the mobile device, receives key information and enables the generation of keys by the TPD. The keys are then sent in a secure manner to the host device to be used for decryption of the broadcast content.

2.7 AOPOC #7: Anonymous Services Access

More and more the “big brother” problem arises in the NTIC society, and is considered by consumers as a potential danger. This POC demonstrates that TPD can be used not only for usual authentication and key management issues, but can also help to enforce privacy considerations, enabling for example anonymous secure access feature.

2.8 AOPOC #8: Biometry

The TPD holds personal data that can be protected with enhanced authentications. Fingerprint recognition is one of them. The TPD is coupled with a passive sensor and computes by itself if the protected data can be accessed.