COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME
ICT Policy Support Programme (ICT PSP)

Towards pan-European recognition of electronic IDs (eIDs)

ICT PSP call identifier: ICT-PSP/2007/1
ICT PSP Theme/objective identifier: 1.2

Project acronym: STORK

Project full title: Secure Identity Across Borders Linked
Grant agreement no.: 224993

D6.0 Pilots Scope

Deliverable Id :	**D6.0**
Deliverable Name :	**Pilots Scope**
Status :	**Final**
Dissemination Level :	**Public-**
Due date of deliverable :	**31 January 2009**
Actual submission date :	**25 February 2009**
Work Package :	**WP6**
Organisation name of lead contractor for this deliverable :	**ATOS ORIGIN**
Author(s):	**Antonio Paradell, Ana Piñuela (ATOS ORIGIN)**
Partner(s) contributing :	**UK IPS, IS MoF, ES CRUE, AT TUG, PT AMA**

Abstract: This document is an overview that describes the scope and objectives of the five pilots.

Project funded by the European Community under the ICT Policy Support Programme

History

Version	*Date*	*Modification reason*	*Modified by*
0.1	23 February 2009	Draft created.	Ana Piñuela, ATOS ORIGIN
0.2	25 February 2009	Milestones included	Ana Piñuela, ATOS ORIGIN
0.3	27 February 2009	Minor changes after quality check	Ana Piñuela, ATOS ORIGIN

Table of contents

List of Figures

List of Tables

Executive summary

Testing cross border recognition of eID and authentication across Europe is at the core of the STORK project.

Extensive testing will take place during several pilots, being part of the work package (WP) 6 of the project. These pilots will create a solid base of testing evidence, because the pilots all refer to real-life services, and include different Member States, different domains (G2B, G2C, G2G, B2B, B2C) and different existing eID solutions.

The pilots defined in this project are:

- *Cross-border authentication platform for electronic services*: This pilot will build a demonstrator showing that cross-border electronic services can operate in a number of Member States. The applications include the UK Government Gateway, the Belgium LIMOSA, the German "service-bw" portal, the Austrian help.gv portal, The Estonian integrated citizen portal, The Portuguese portaldocidadao.pt portal and the Catalan Public Administrations Portals.
- *SaferChat*. The main objective of this pilot is to build a platform for safer online environment where people can communicate on-line using their eIDs and demonstrate its use.
- *eID Student mobility*. The main objectives of this pilot are to facilitate students' mobility across Europe.
- *eID Electronic delivery*. The objective of this pilot is to demonstrate cross-border electronic delivery based on the existing domestic infrastructure.
- *Change of address*. This pilot will test the electronic process of address change of EU citizens that move abroad to other Member States.

In order to have a common view of all the pilots a new list of deliverables has been elaborated. The aim of this list is to deliver the same documentation for all the pilots:

D6.0 – Scope of the pilots

D6.x.2 – Pilot specifications

D6.x.3 – Interim report (just before going online)

D6.x.4 – Pilot progress (short status on the running pilot)

D6.x.5 – Final Report (final status on the running pilot)

The first deliverable, D6.0, provides an overview document of the five pilots with their goals, scope and milestones.

1 Introduction

The objective of WP6 is to run a number of eID interoperability pilot services to implement and test the common specifications defined in WP5. This will be achieved as an iterative process, starting with the initial common specifications from WP5, implementation of the pilots and evaluation with feedback for the specifications. The pilots will run for a period of one year.

The objectives can be summarized as follows:

- implementation and demonstration of the interoperability services;
- operations between cooperating Member States in the context of the pilots described in this WP6 taking as starting point the services that are already operational at national level;
- final implementation of an open, common interoperable service solution based on an initial common specification agreed amongst participants in the pilot. During the course of the pilot the initial common specification will be further developed and gain a wider agreement in view of eventual scalability.

The following pilots will be validated during the project life:

- 6.1 Cross-border authentication platform for electronic services
- 6.2 Safer chat
- 6.3 eID Student Mobility
- 6.4 eID Electronic Delivery
- 6.5 Change of address

2 Pilots

2.1 Cross border authentication platform for electronic services

2.1.1 Goals

The Cross Border Authentication for Electronic Services (WP6.1) will *deliver applications (Service Providers) showing that cross-border electronic services can operate in a number of Member States.* In order for these applications to function they need to be connected to the EU interoperability layer defined by the common specifications of WP5.

The objectives of this pilot are:

1. To test and implement the trust framework defined in WP2 by operating services requiring different authentication levels.
2. To test with applications and national eID systems the EU interoperability layer defined and implemented in WP5.
3. To connect existing national portals and services participating in the Cross-border authentication platform for electronic services to the EU interoperability layer and the reference architecture models defined in WP5
4. To test that the connections function with a variety of log-in methods and tokens.
5. To assess ease of use and take-up of cross-border e-ID services
6. To implement an EU portal providing a series of links to all the services accessible within the WP.

2.1.2 Scope

In order to deliver against the objectives defined above it was necessary for each Member State to commit to a high level scope within for the Pilot.

The table below shows which Member States are engaged in WP 6.1. It also shows the high level view of the agreed involvement that has been positioned by each Member State. This agreed involvement is defined as whether the Member State will provide an online application (service provider) to be accessed and / or enable their national eID credentials to be used within the pilot.

The agreed involvement can be seen in the table below.

Member State	Service Provider	EID Credentials
Austria	help.gv.at	ID Card,
Belgium	Limosa.be	N/A
Estonia	eesti.ee	ID Card, Mobile Phone
France	n/a	ID Card
Germany	mein-service-BW	ID Card , User ID and Password
Netherlands	n/a	User Name, Password and SMS

		Token
Portugal	portaldocidadao.pt	ID Card
Spain	Catalan Portal	ID Card, idCAT
UK	direct.gov.uk	User ID and Password

Table 1: Level of involvement from each Member State in the pilot

The scope of the pilot includes the connection of the services to the Interoperability layer being delivered by work package 5 but not the connection of the eID credentials to the interoperability layer. This will be delivered by work package 5.

Many of the Member States service providers will be either national or local portals or the entitlement to services within these portals will be controlled by the portal themselves. For instance, the Limosa service is a service in its own right and it is concerned with the right to work in Belgium. The role of the pilot is to ensure that the Citizen is authenticated with their appropriate eID, to the appropriate trust level, for access to the service.

The service providers offer the follow services within their environments:

Austria - help.gv.at

- personalised services and information, with a personalised profile, using forms which are in part already filled in,
- their own directory of relevant authorities,
- a personalised reminder service,
- electronic delivery services
- links to other Portals provide one-stop-shopping as far as possible

Belgium – limosa.be

- Enrolment into the service for right to work in Belgium.

Estonia - eesti.ee

- Registration
- Company official e-mail forwarding
- Send e-mail from company official e-mail address
- Send e-forms to Estonian public sector institutions
- Track sent e-forms statuses

Germany - mein-service-BW

- Registration to mein-service-BW as registered user
- customize service-BW to your previously entered filter criteria.
- full functionality of mein-service-BW

Portugal - portaldocidadao.pt

- General portal services

Spain – Catalan Portal

- applications of public administrations in Catalonia.

UK – Directgov (Government Gateway)

- Enrolment into any available service with the use of UK issued identifiers.
- Depending on timing this will either be the direct.gov.uk portal or the UK Government Gateway at gateway.gov.uk.

2.2 Safer Chat

2.2.1 Goals

The main objective of the Safer Chat pilot (WP6.2) is to *build a platform for safer online environment where people can communicate on-line using their eIDs and demonstrate its use in a comprehensive pilot project.*

The Internet is a great way of staying in touch and meeting people, both for leisure and business. Chat rooms, blog, MSN and email make it easy to communicate with people from all over the world. However, the net can also be used for inappropriate communication; this includes for example approaching children with illegal and harmful intentions or online identity theft. Thus, it is important to explore all possible means in order to make online communication as safe as possible for children; simultaneously, the pilot results will be beneficial to all users.

The pilot will have the following goals:

- Build a platform for safer online communication using eIDs
- Demonstrate, in a pilot, the use and benefits of eIDs in this relation
- Test the interoperability specifications and solutions provided by WP5
- Consolidate results and draw conclusions

2.2.2 Scope

Safer chat is aimed to make chat rooms more secure where people use their eIDs for identification/authentication/authorization.

The following countries participate in this pilot:

- Austria
- Belgium
- Iceland

It is foreseen to use already proven Safer chat solution that both Belgium and Iceland has been using. Austria will amend children and school platforms with the interoperability layers to allow

for eIDs. These solutions will then be adapted to make use of the specification and solutions from WP5 to gain support for different eIDs from different countries. Apart from using an eID to access to these chat rooms access can be limited by attributes such as age and gender. The solutions should have well defined and easy ways of adding new limits to the chat room.

The pilot will make use of eTwinning, a framework for schools to collaborate over the Internet with partner schools in other European countries. This is an already established framework that has representatives in each country which promotes eTwinning nationally. In this framework, pupils and teachers will make use of this new solution and work on certain projects. One of them is to develop chat rooms for kids that they think kids will use. One of the biggest challenges is to get kids to make use of this new way to communicate. Because of that it is important to get kids involved in making this accessible for their piers, kids to develop for kids. The kids will also work on Educational packet on safer internet use.

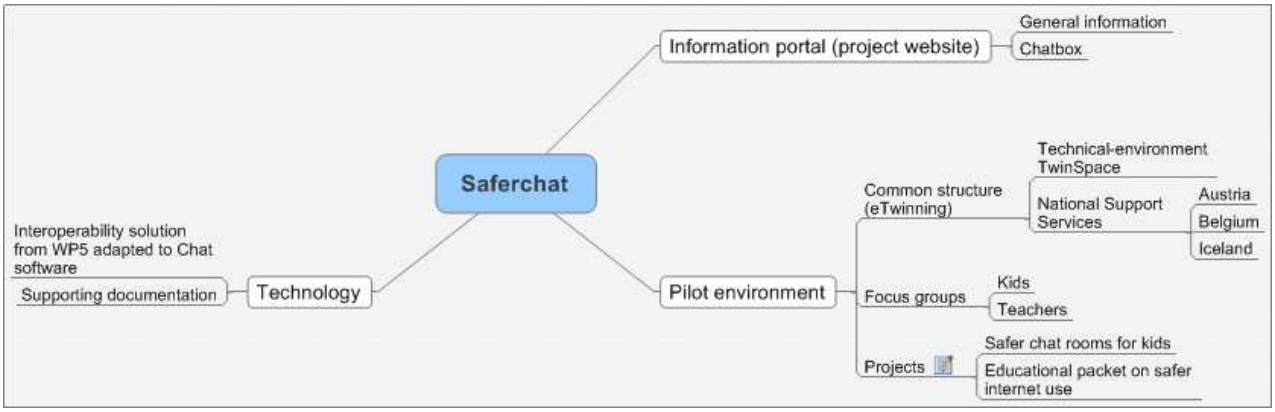

Figure 1: Safer Chat conceptual architecture overview

2.3 eID Student Mobility

2.3.1 Goals

The objective of this pilot (WP6.3) is to *facilitate students' mobility across Europe. It will mainly enable foreign students to get access to any on line administrative service offered by a particular University using their national eID card of origin for eIdentification or eSignature purposes.*

2.3.2 Scope

The scope of STORK work package 6.3, Students' Mobility Pilot, is oriented towards facilitating students' mobility across Europe. This objective is addressed by enabling foreign students to access on-line University's administrative services using their own national electronic identity (eID). Universities involved in the pilot provide many different eServices to their students. However, the pilot to be carried within WP 6.3 will put the focus in the enrolment/pre-enrolment of foreign students and in the problem of identifying and authenticating them. Access to other academic eServices, such as on-line courses and tutorials, profile specific information or on-line assessment and consultation of academic information remain will be a secondary objective and will be granted as a result of the enrolment/pre-enrolment process.

In order to guarantee the success of the pilot and cope with the potential risk of a limited number of students taking part in it, *two different scenarios* have been considered. These scenarios have different complexity.

- One of them is intended to provide access to students with a valid STORK identity to on-line enrolment/pre-enrolment processes put at their disposal by Universities participating in the pilot.
- The second one reflects a slightly more complex approach to academic enrolment and includes the role of Universities involved in the pilot as attribute providers that will be able to add academic information linked to the student following a *European Supplement to the Degree* format.

The role of Universities in this pilot can be summarized as follows:

- **Services Providers (SPs):** In all cases Universities act as services providers. At least a pre-enrolment/enrolment e-service should be put at the disposal of foreign students.
- **Attribute Providers (APs):** An additional value for the pilot could be obtained by the fact that Universities become also providers of some academic data linked to the identity of the students (*European Supplement to the Degree)*.

Student's mobility pilot has several concerns related to interoperability. In some cases, the eService provider **(SP)** only needs confirmation that the user accessing a concrete electronic service is who claims to be. In other cases, a more efficient service could be offered to foreign students if they allowed their University of origin to provide full data on the academic record of the student (e.g.: European Diploma Supplement, Europass,…).

The pilot prepared in work package 6.3 focuses on identity aspects, i.e. the question of how to identify and authenticate individuals for granting them access to academic services, but also keeps in mind that a student's identity may contain many different attributes related to the academic background.

Following these premises, two different use cases have been formulated:

- **Use Case 1:** STUDENTS ACCESS TO UNIVERSITY SERVICES

  It considers a simple exchange of basic identification data. Additional documentation, if needed, should be later provided to the destination university, that is, academic degrees or any additional data that could not be provided by STORK.

  Any citizen with a valid STORK credential would be able to use this service.

- **Use Case 2:** STUDENTS ACCESS UNIVERSITY SERVICES AND UNIVERSITY VALIDATES INFORMATION FROM UNIVERSITY OF ORIGIN

  A slightly more complex exchange of data is considered. In this use case, the university of origin provides, in addition to basic data, a document (signed or not) that will be checked by the university of destination.

  In this case, the information needed will be provided by Universities participating in the pilot from Portugal, Italy, Austria and Estonia, and by Spanish Universities included in the CRUE-TIC Electronic Administration subgroup.

All participants should be able to implement at least the simplest use case. The STORK Students' Mobility pilot is intended to demonstrate interoperability in a practical and useful way. After having a detailed pilot specification, each participating academic institution will decide its achievable interoperability level according to its possibilities and other technical, legal or organizational issues.

2.4 eID Electronic Delivery

2.4.1 Goals

The objective of this pilot (WP6.4) is to *demonstrate cross-border electronic delivery based on the existing domestic infrastructure. It is essential for e-Government to conclude transactional processes electronically and inter alia also requested by the Service Directive to be able to transact administrative procedures fully electronically.*

2.4.2 Scope

The scope of STORK work package 6.4, the e-delivery pilot, is to *provide a concept for an interoperable e-delivery framework.* Work package 6.4 explicitly concentrates on identity related issues thus deals with the e-delivery process in general and focuses on how to identify and authenticate involved entities in all phases of e-delivery. Legal aspects are addressed in an analytic way.

With respect to the given legal situation, work package 6.4 claims to identify problems and highlight possible approaches to solutions, but does not aim to effect national legislations. In order to run the 12 month pilot-phase successfully, a pragmatic legal arrangement is envisaged.

E-delivery touches many facets with respect to interoperability. However, the pilot prepared in work package 6.4 explicitly focuses on identity aspects, i.e. the question of how to identify and authenticate entities during sending and receiving of deliveries. All other issues, such as the interoperability of e-documents, etc., are not the primary scope of work package 6.4. These issues are only addressed as far as necessary for a successful pilot phase.

Considering cross-border e-delivery use-cases, the following scenarios can be identified being the basic e-delivery scenarios which are relevant for STORK and this pilot. The scenarios are sorted following increasing complexity; thus the first scenario—Level 0—is the domestic e-delivery scenario (see Table 2: Basic scenarios and their complexity levels).

- **Level 0:** A citizen of Member State A registers with an e-delivery portal of Member State A using her eID. As a result, the citizen is able to receive deliveries from senders of Member State A through the e-delivery portal of Member State A (domestic scenario).
- **Level 1:** A citizen of Member State A registers with an e-delivery portal of Member State B using her eID. As a result, the citizen is able to receive deliveries from senders of Member State B through the e-delivery portal of Member State B.
- **Level 2:** A citizen of Member State A registers with an e-delivery portal of Member State B using her eID. As a result, the citizen is able to receive deliveries from senders of any participating Member State C through the e-delivery portal of Member State B.

The STORK e-delivery pilot aims to demonstrate e-delivery scenarios of all levels. After having a detailed pilot specification, each participating Member State will decide its achievable interoperability level according to the legal, technical and organisational findings.

Level	Citizen (Receiver)	e-Delivery Portal	Sender
0	MS A	MS A	MS A
1	MS A	MS B	MS B
2	MS A	MS B	MS C

Table 2: Basic scenarios and their complexity levels

The following countries participate in this pilot[1] (in alphabetical order):

- Austria
- Luxembourg
- Slovenia

Slovenia and Austria have a domestic e-delivery infrastructure in place already; Luxembourg has recently started their e-delivery framework.

Furthermore, in order to broaden the discussion work package 6.4 seeks for further interested affiliated contributors and partners. Therefore, work package 6.4 has started the dialog with developers and providers of other e-delivery frameworks from the very first moment. As a result, developers and providers of the German DE-Mail System could be gained being an "affiliated partner" with work package 6.4, which means that they are involved in conceptional and technical discussions from the very first moment.

The scope of work package 6.4 is focused on the identification of entities—i.e. natural and legal persons—during all processes of e-delivery. The processes of registration of receivers and addressing/finding of receivers (in the course of sending) are of major importance.

Furthermore, interoperability issues of the entire e-delivery process are addressed by work package 6.4, in particular relating to

- sending of e-deliveries, whereas sending could be
  - initiated by government with and without knowing the receivers electronic address in advance (the receivers e-ID must be known in either case)
  - initiated by other parties, e.g. the private sector
- receiving of e-deliveries, whereas the following issues are of paramount importance:
  - notification of receivers
  - qualified proof of delivery

Work package 6.4 is analysing the given legal requirements in order to identify problems and to sketch attempts to solutions. Important legal issues are:

- the time-limit for taking up deliveries (depending on national legislation)
- the form of receipts (qualified proof of delivery)
- and the different qualities of deliveries (depending on national legislation)

The achievement of full interoperability of e-delivery systems and all its facets, for example, regarding e-documents, signature formats, etc., is out of scope of work package 6.4. These interoperability issues, especially the interoperability of e-documents for instance, are subjects of other projects and Large Scale Pilots. Furthermore, this pilot does not aim to effect national legislation. Instead, work package 6.4 will identify legal issues and problems, but aim to seek for pragmatic solutions with respect to the 12 month pilot phase.

.

Within the first 9 month work package 6.4 aims to develop an interoperability concept for the domestic e-delivery systems of work package 6.4 partners, i.e. Luxembourg, Slovenia and Austria. In the course of developing the concept, this work package plans to create an inventory which should provide an overview of existing e-delivery approaches and thus a common

[1] Estonia is also a partner in WP6.4. However, Estonia will not participate in the pilot.

understanding of requirements. While the e-delivery systems of Luxembourg, Slovenia and Austria are the primary focus of the inventory, it is not limited to them. However, the inventory is rather a tool for creating the concept than an official deliverable.

The resulting interoperability concept will address the following two main aspects:

(1) how the administration gets hold of the electronic address of the addressee and

(2) how a qualified proof of delivery that is returned to the sending administration is established.

Based on the concept, a detailed specification will be developed. The specification is the basis for all technical implementations required for the e-delivery pilot. It incorporates comments received from the discussions on the interoperability concept, but also establishes a minimum specification of electronic documents that can be electronically delivered cross-border during the pilot-phase.

The major elements of the specification are the definition of interfaces und e-delivery processes. Therefore, the specification includes interfaces to determine whether a citizen given her electronic identification can be reached by electronic delivery, to deliver an e-document electronically, and the specification of the electronic notification of receipt. The resulting specification should serve a basis for the implementation of modules required for the pilot phase.

Using the specification, work package partners will start to develop interoperability modules and converter required for cross border delivery. The envisaged procedure is that when the electronic address of the citizen has been determined, the electronic document is delivered and a notification of receipt is returned. As the national solutions differ technically, converters need to be developed and tested. A proxy or gateway approach is followed where transformation of the national delivery system to the foreign one takes place at dedicated converters.

For integrating citizen authentication to pick up the delivered documents the interoperability modules developed in work package 5 are used. However, these modules and converter have to be finished and put in place until M22 as with M22 the pilot phase is planned to start.

2.5 EU Citizen Change of Address

2.5.1 Goals

The objective of this pilot (WP6.5) is to *test the usage of eID authentication to support the electronic process of address change of EU Citizens that move abroad to other Member States.*

This pilot objectives are:

- Detail definition of the EU Citizen Change Of Address process
- Specification of Address Canonical Data Model
- Specification of Change of Address Service Provider and User Interfaces
- Technological Implementation of MS Service Providers and User Interfaces
- Technological Integration with the eID Common Infrastructure
- Change of Address Tests
- Run Real life pilot
- Consolidate results and draw conclusions

2.5.2 Scope

The establishment of free circulation of individuals within the European Union and the extension of its borders generated by the enlargement process has fostered the mobility of citizens. However, citizens that exercise their right to move to another EU country sometimes face a considerable amount of bureaucracy and time wasting procedures, necessary to inform several entities (either in is origin country or others) of his new address. Besides resulting in another obstacle that the citizen has to overcome, this situation usually creates incoherence on the address data known to each MS especially when a citizen fails (with or without intention) to notify one of them.

Thus, and taking advantage of the increasingly widespread of eID across the European Union, this pilot aims to *allow a citizen to notify all the relevant[2] MS of his new address as a result of a single request, conducted through the Internet and authenticated with his eID*. That request will be interpreted by a Service Provider deployed by each MS participating in the pilot that, after performing the adequate validations, will notify the Service Providers of additional MS and orchestrate the defined process, in order to ensure that the citizen is authenticated, that the information is accurate and that there are no incoherencies between different MS.

To achieve the pilot's goals, a process to support the communication and coordination between two or more different MS will be proposed. This process will be terminated internally by each participating MS, each one with its own set of rules. With this approach there is no transaction coordinator. The transaction is coordinated by the Change of Address (CoA) service that initiated the process.

Therefore, the model will use a generic approach to leave space to each MS to fit its own set of rules. To accomplish this, the following conditions will be established:

- Pre-Conditions – that are verified by the destination MS before the CoA process. Only after the citizen fulfills the pre-conditions the process can begin;
- Post-Conditions – are verified just before the process ends. If the destination MS has requirements which have to be fulfilled before the process finalization (e.g. address confirmation), just report them and, after the requirements are fulfilled, notifies the CoA service that initiated the process.

The following figure provides an overview of the process to be discussed:

[2] For instance, the MS where the citizen is moving into, the MS that issued the citizen's eID, another MS where the citizen has worked in the past, etc.

Figure 2: Main Flow of the CoA Process

Whenever post-conditions are put in place, the CoA commit process flow will have to be observed. So, when the destination MS has requirements that the citizen has to fulfil, the CoA process is put on wait. When those requirements are met, the following flow is executed:

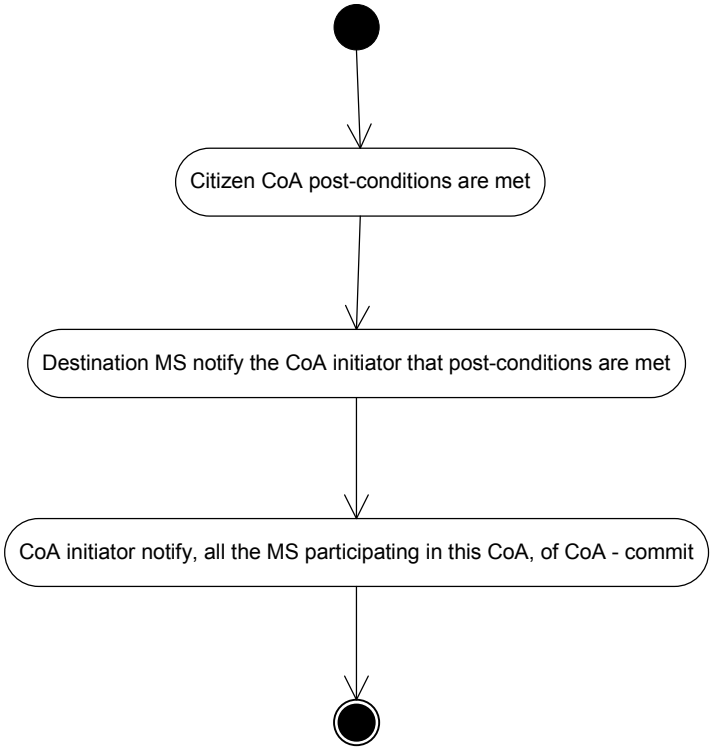

Figure 3: CoA Process Commit Flow

3 Milestones

In order to run the pilots successfully the following milestones have been identified (they are common for all the pilots):

Key Milestones	Start Date	Due Date
Scope of pilots High level document, what are we trying to achieve		January 2009
Identification of use cases		January 2009
Definition of use cases		January 2009
Definition of acceptance criteria - Project level for the EC - Testing level	February 2009	
Definition of the Business Model of Pilots - Requirements regarding Trust Levels - Requirements regarding eIDAttributes for Service Provider	February 2009	
Definition of the interfaces of each Service Provider to the common layer Dependency with common specification (WP5) and internal decision on architecture deployment		May 2009
Each Member State to decide whether to support PEPS and/or MW including tokens, ID Providers and Attribute Providers		May 2009
Testing - Test Method WP6.0 - Test Cases 6.1 …. 6.5	February 2009	
Definition of the model that shows interoperability between Service Provider, ID Providers for each pilot	February 2009	
Test Plan for each Service Provider including those Member State that do not have ID Providers - One for each pilot	February 2009	
Definition of the user interface for authentication		May 2009
Service Modifications to integrate to common layer	May 2009	October 2009
Interoperability Test Planning - Run by WP5.3	May 2009	
Connection to the common layer for testing	October 2009	
Individual Service Provider testing against common layer - Coordinated at national level	October 2009	
Interoperability Testing - At Member State Level	December 2009	

- Coordinated by WP5.3		
Define minimum position to be able to go operational	QTR2 2009	
Post go live planning – Evaluation, - Communication, - Sustainability	QTR 2009	
Interoperability Layer Decision -> MS Council WP5 will provide a technical assessment after doing the interoperability testing to the MS Council	February 2010	
Identify, manage risks -> Review before going live -> MS Decisions Process for what to do in disagreement	March 2010	
Connection of all the services to the production interoperability layer	March 2010	
Production Testing - Running the pilot over the Internet - Testing before advertising people	March 2010	

Table 3: Milestones of the pilots