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

Towards pan-European recognition of electronic identities (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

List of Commission A2A Services of Common Interest

Deliverable Id :	**D7.3**
Deliverable Name :	**List of Commission A2A Services of Common Interest**
Status :	**FINAL**
Dissemination Level :	
Due date of deliverable :	**M6**
Actual submission date :	
Work Package :	**7.1**
Organisation name of lead contractor for this deliverable :	**AT BKA**
Author(s):	**Hubert Schier**
Partner(s) contributing :	

Abstract: This document aims to identify a way how to incorporate the findings of STORK into the A2A services operated by the European Commission. Several of these services of common interest are described by way of example, and special attention is devoted to the European Commission Authentication System (ECAS).

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

History

Version	*Date*	*Modification reason*	*Modified by*
1.0	26.08.2008	initial draft	HS
1.1	28.10.2008	updates in sections 2.1, 2.2, 2.3 and 2.5	HS
2.0	19.11.2008	new chapter 3 about ECAS new chapter 4 Conclusions	HS

Table of contents

Executive summary

This document aims to identify a way how to incorporate the findings of the EU co-funded project STORK into the A2A services operated by the European Commission for itself and for the Member States. Several of these services of common interest are described in the following by way of example, and special attention is devoted to the European Commission Authentication System (ECAS) in chapter 3, which could possibly be the starting point for including electronic identities into the username/password solutions which are currently still the commonly accepted access method for ICT systems.

1 Introduction

1.1 Scope and objectives of the deliverable

The European Commission i2010 eGovernment Action Plan stated that eID solutions will be key enablers of secure and seamless access to modern public services. Ensuring the availability of an electronic identity management (eIDM) backbone across Europe will help to serve the citizens and businesses in their interaction with governments.

The eID Large Scale Pilot STORK aims to develop not only a shared vision to align actors in the field, but also pilot trans-border eGovernment identity services, as well as to learn from practice on how to roll out such services, and to experience what benefits and challenges an EU wide interoperability system for recognition of eID will bring.

The project will

- contribute to accelerate the deployment of eID for public services, while ensuring co-ordination between national and EC initiatives in the field and support federated eID management schemes across Europe
- test, in real life environments, secure and easy-to-use eID solutions for citizens and business, in particular SMEs and government employees at relevant levels (local, regional, cross/national level)

The scope of the deliverable at hand is defined in the Description of Work (DoW) as a sub-task 7.1 of Work Package 7.

Applications of "common interest", i.e. in the interest of the European Commission as well as of Member States, are first to be identified. This will be done in close cooperation with Commission Services. Next, common specifications will be derived by the WP participants (deliverable 7.4). Implementation will be carried out by the Commission Services and is not funded under the STORK project. Finally, a report on the implementation process will be produced (deliverable 7.5).

In detail: in contrast to citizen-oriented communication, this deliverable does not only involve subgroups of the MS participating in the Pilot and the specific applications run by them; instead it concerns the profits to the EU27 as a whole, since these applications are operated by the Commission – or other European Institutions – for all MS alike. eID is offered as an additional feature for enhanced security.

The European Commission provides various A2A services with restricted access rights. Currently, these are often handled by a rather insecure system using e-mails, usernames and PIN/passwords. With the Service Directive in particular, Europe is facing a major eID challenge. A seamless identification of users, as well as of government officials, needs to be in place. For this purpose, it is crucial that the common services are integrated and that they use "European eID interoperability".

1.2 Methodology

A first list was drafted using Section I of the IDABC Work Programme 2008 describing projects of common interest and horizontal measures. This work programme is co-ordinated and aligned with related Community programmes such as the CIP. Horizontal measures develop the components of the infrastructure for cross-border service delivery while the specifications for the overarching structure are being prepared. See in particular the Common Identity Management Service (CIMS) described in chapter 3.2 of the document, and the following chapter on eID interoperability.

IDABC projects and horizontal measures focus on the implementation of operational services and infrastructures. They take into account, whenever appropriate, the results of the innovative and exploratory projects and pilots and of the studies undertaken in the related Community programmes.

Existing EC systems as well as projects in different stages of planning, implementation or testing have been selected from reference [1] depending on whether they feature particular needs for reliable authentication of users and/or contents. When considering these systems from the user and service perspective, confidentiality (i.e. access control) and integrity (i.e. risk of data alteration through unauthorised access) could be guaranteed by ensuring that appropriate authentication (and possibly also authorisation) mechanism be put into place. An interoperable authentication or identity management mechanism that could span across different domains (national or EU Institutions) is clearly the target solution. Most of the services listed below have already expressed their intention of using additional security measures as described in the IDABC Work Programme.

This list of services does of course not pretend to be exhaustive, and can be complemented at any time in the future. Suggestions have e.g. been made to include electronic travel reimbursement and some other internal "housekeeping" systems, which doubtlessly are of common interest and have a certain amount of authentication needs.

Reference [1] gives few information about the approximate number of real or potential users for most systems, but names at least the units and the persons in charge, who have been asked to comment on the document and to provide additional input. Regrettably, less than 50% of the EC services concerned have replied to this request. A meeting which was organised in Brussels to discuss the issue was attended by DG MARKT, DIGIT and EMPL.

1.3 Reference to related work packages

Since the objectives of Working Package 7 are to communicate and promote the methodology and findings of STORK, it will in a way get input from the entire project, but especially from WP5 (common specifications) as far as task 7.1 is concerned. The subsequent deliverables have already been described above.

2 Commission A2A Services of Common Interest

2.1 Internal Market Information System (IMI)

Objectives:

The fundamental objective of the Internal Market Information (IMI) system is to create the conditions in which day-to-day administrative cooperation between Member States can take place, by supplying a cross-border e-government application to support Internal Market legislation. The system is an enabling mechanism. It will provide Member State administrations with a multilingual, open and flexible tool with interfaces to other European and national IT-applications and databases (where applicable) to support the mutual assistance and information exchange required to implement Internal Market legislation efficiently. The system shall be operated and maintained by the Commission. IMI will overcome barriers to cooperation created by different administrative cultures, structures and languages and will provide clearly identified partners and procedures. European citizens and businesses will be able to rely on a fast and constructive response by administrations to help cross-border activities and enable them to take advantage of Internal Market opportunities.

The responsibility for implementing and ensuring compliance with the legislation, in practice, lies with a large number of public authorities in the 27 Member States. These authorities must be in a position to cooperate closely. However, different administrative cultures, structures and languages as well as a lack of agreed procedures and clearly identified partners are significant barriers to Member States working efficiently together.

A Competent Authorities database will be built up gradually, beginning with those authorities who will use IMI to exchange information according to their obligations under the revised Professional Qualifications Directive. A beta version of IMI is intended to pilot with 4 professions (accountants, doctors, pharmacists and physiotherapists). In following phases IMI will be further enhanced to support the specific requirements of the Services Directive.

Service in charge: MARKT.E.3

Associated service: DIGIT, DGT

Responsible action manager: LEAPMAN Nicholas

Committee/group of experts: Internal Market Advisory Committee (IMAC)

User group: Member States competent authorities for Services and Professional Qualification Directive; currently around 400, up to 100.000 potential authorities when fully operational

Current authentication methods: username / password / 12-digit pincode

2.2 Communication and Information Resource Centre for Administrations, Business and Citizens (CIRCABC)

Objectives:

Continuation of project CIRCA, which provided information pages, documents repository, search and retrieval, directory and access management, meetings organisation and newsgroups/discussion fora.

The existing user community is very large and the service is considered as critical by many committees and workgroups. In 2007, over 17.000 users participated to around 1.150 active Interest Groups with an average number of 9.000 users connecting every week.

Hosting and supporting a service which improves collaboration between committees and working groups involved in projects of European Union Institutions and Member State administrations at pan-European level, the new system will also improve interactivity between administrations and citizens as well as interactions between businesses and citizens. Multilingual aspects and security features are currently added.

Service in charge: DIGIT.A.3.EGIS

Associated service: ESTAT, MARKT, OPOCE

Responsible action manager: WEISSENBERGER Jean-Marie

Committee/group of experts:
Pan-European eGovernment Services Committee (PEGSCO)

User group: Yearly stakeholders conference; internal Steering + Technical Committee

Current authentication methods: ECAS (EC Common Authentication Service) which enables Web applications to authenticate centrally. It offers also single sign-on between applications using it. It includes CAS software developed by Yale University.

2.3 Electronic Exchange of Social Security Information (EESSI)

Objectives:

The social security coordination rules are applied and put into practice through exchange of information between social security institutions of the Member States and the EFTA states. This means that, in order to guarantee appropriate and correct protection of the social security rights of citizens who are mobile, there is a permanent, regular and complex flow of information between thousands of social security institutions in the Member States, comprising mainly information on validity of rights, insurance history, competent social security institutions, identification of the citizen and payment of benefits and contributions.

As a matter of fact, the bulk of these exchanges is still done by sending paper forms in 22 different language versions. IT-based exchanges would permit and lead to:

- improved knowledge on the quality and reliability of the data
- increased use of the data
- multiple usage of the data
- efficient verification of the data
- faster processing
- more flexible and easier interface between different systems

Data protection and privacy aspects are of course of major importance in this context.

Service in charge: EMPL.E.3

Responsible action manager: RAI Shahida

Committee/group of experts:
the Administrative Commission for social security for migrant workers, and in particular the Technical Commission on Data Processing

User group: social security clerks in national administrations

Current authentication methods: to be determined (call for tender for the system has been launched this year)

2.4 DG SANCO Reference Database System (SANREF)

Objectives:

Within the area of Food Safety, most networks have the need to contain and maintain reference information. This has lead to the situation where many networks contain and exchange the same type of information but in a different format or structure, which doesn't allow for easy creation of global reports or lateral cross-checking across systems. In addition, it forces most projects to re-invent a reference data model and to develop a user interface to maintain such information, which is inefficient.

The new Feed and Food control regulation establishes the need to have a correct cross-checking option of reference information across the Food Safety policy area. SANREF will store and provide interfaces to Food Safety reference information. Existing and new networks will be able to use the interfaces within their applications. This includes:

- Member States administrations
- Member States authorities
- Member States institutional structures
- Economic Operators within Member States having a relationship with the Commission
- Members of the public having interaction with the Commission
- Other relevant organisations

Service in charge: SANCO.A.4

Responsible action manager: BRAND Herman

Committee/group of experts:
Standing Committee on the Food Chain and Animal Health (SCFCAH) - IT working group

User group: *information not provided*

Current authentication methods: *information not provided*

2.5 Consumer Protection Cooperation System (CPCS)

Objectives:

A recent Regulation enables the competent national authorities to cooperate in detecting, investigating and stopping, if necessary through the courts, businesses that break the laws protecting the economic interests of consumers. Each of the authorities involved will be

able to call on other members of the network for assistance in investigating possible breaches of consumer laws, and take action against rogue traders.

The three main objectives of the CPCS are:

- to act as a secure central repository of information, to be accessed by the competent authorities
- to act as a secure communication system between the authorities
- to include remaining functionalities that are necessary to allow for a proper execution of the actions defined in the Regulation and satisfy specific authorities needs

In order to adapt the application to be completely in line with the data protection regulatory framework, additional implementation work will have to be done.

Service in charge: SANCO.B.5

Responsible action manager: JANSCHEK Maria Luisa

Committee/group of experts:
Consumer Protection Cooperation Committee

User group:

There are mainly two types of users:

- Case handlers in the Competent Authorities designated by the Member States as being responsible for the application of at least one of the Legal Acts listed in the Consumer Protection Cooperation Regulation (EC) 2006/2004
- Officials working in the Single Liaison Offices, i.e. the authority responsible for the coordination of the application of Regulation (EC) 2006/2004 in a given Member State

In addition to the above, the Commission has a restricted access (consultation only) to some of the information exchanged between authorities.

Current authentication methods:

The CPCS is only accessible to authorities through the sTESTA network. No access from the internet is allowed.

Access is only granted to the public enforcement authorities formally designated by the Member States and to nominative users (i.e. 'competent officials' pursuant to article 3 of Regulation 2006/2004). Password rules are: initial password is given to user and must be changed with first login. Strong password form is used.

CPCS uses the SANCO-wide authentication and authorisation system (SAAS-SANCAS). SAAS-SANCAS is ECAS-compliant and is designed to evolve toward the use of electronic certificates for authentication. It could probably serve as a service in the context of the use of eID infrastructure.

Particular care should be given to real usable systems, while the older attempts to such projects collapsed because the internal Commission services (namely ADMIN-DS and DIGIT) were not involved early enough in the project, thus no platform could be deployed or management of the Ids organised.

2.6 LISFLOOD-ALERT

Objectives:

This is a harmonised on-line information system, updated in real time, capable of providing an early alert on potential floods to the relevant civil protection and water authorities in the Member States, thus improving the ability to respond appropriately and in time.

The scope of the project is to create a data environment that allows flood forecasting with larger lead times in large river basins, where downstream forecasts rely on the availability of upstream river flows and observed and forecasted meteorological data.

Throughout Europe, this information is not or only scarcely available, and whatever is available is scattered over more than 75 authorities. Therefore, the aim is to establish a harmonised system for exchanging these real-time water level and river discharge data between Member State administrations and the organisation running the European Flood Alert System.

The potentially larger lead times will increase the preparedness of national and regional water authorities and civil protection services. This increased preparedness and furthermore increased warning time potentially reduces the number of flood victims and reduces a part of the flood damage by timely evacuation.

Service in charge: JRC

Associated service: ENV.A.3

Responsible action manager: DE ROO Arie

Committee/group of experts:
Management and Regulatory Committee for Civil Protection (MRCCP)

User group: *information not provided*

Current authentication methods: *information not provided*

2.7 European Competition Network - Electronic Transmission (ECN-ET)

Objectives:

In the context of the competition rules, the Commission services have the duty to transmit to the Member States documents which are relevant for the assessment of specific cases. Due to the confidentiality of some documents, security is a fundamental point to be managed in this system. The use of ECN-ET will be restricted to the competition authorities involved.

Service in charge: COMP.R.3

Associated service: COMP.A.5, COMP, DIGIT

Responsible action manager: PEREZ ESPIN Manuel

Committee/group of experts: European Competition Network Committee

User group: *information not provided*

Current authentication methods: *information not provided*

2.8 European Database for Medical Devices (EUDAMED)

Objectives:

The system is accessible to competent authorities to register manufacturers, medical devices, certificates and incident reports, either manually or by uploading them from their national databases. This creates the possibility for market surveillance and warning capabilities. The medical devices sector will have access to products information and vigilance reports, leading to increased protection of Public Health.

Service in charge: ENTR.F.3

Associated service: ENTR.R.3

Responsible action manager: *information not provided*

Committee/group of experts: Medical Devices Expert Group (MDEG)

User group: *information not provided*

Current authentication methods: *information not provided*

2.9 Secure Exchange and Storage of Agricultural Data (SESAD)

Objectives:

Data pertaining to agriculture circulates between the Member states and the DG AGRI on a daily basis. Though this data itself is not "EU classified", there is a growing need to ascertain that the data being sent is not tampered with and that the sending users are really who they pretend to be.

As most of the financial data transfer between MS correspondents and the DG AGRI is nowadays done using electronic means (electronic messages and/or submission of Web forms), a high level of security and integrity must be guaranteed. This "securisation" of the transferring will also allow DG AGRI to reduce the paper circulating between MS and the Commission, by replacing an important number of paper reports by electronic data submission.

Service in charge: AGRI.I.3, AGRI.I.4, AGRI.D.2

Responsible action manager: KOORNSTRA Timotheus

Committee/group of experts:
European Agricultural Guidance and Guarantee Fund Committee (EAGGF)

User group: *information not provided*

Current authentication methods: *information not provided*

3 The European Commission Authentication Service (ECAS)

3.1 What does it do?

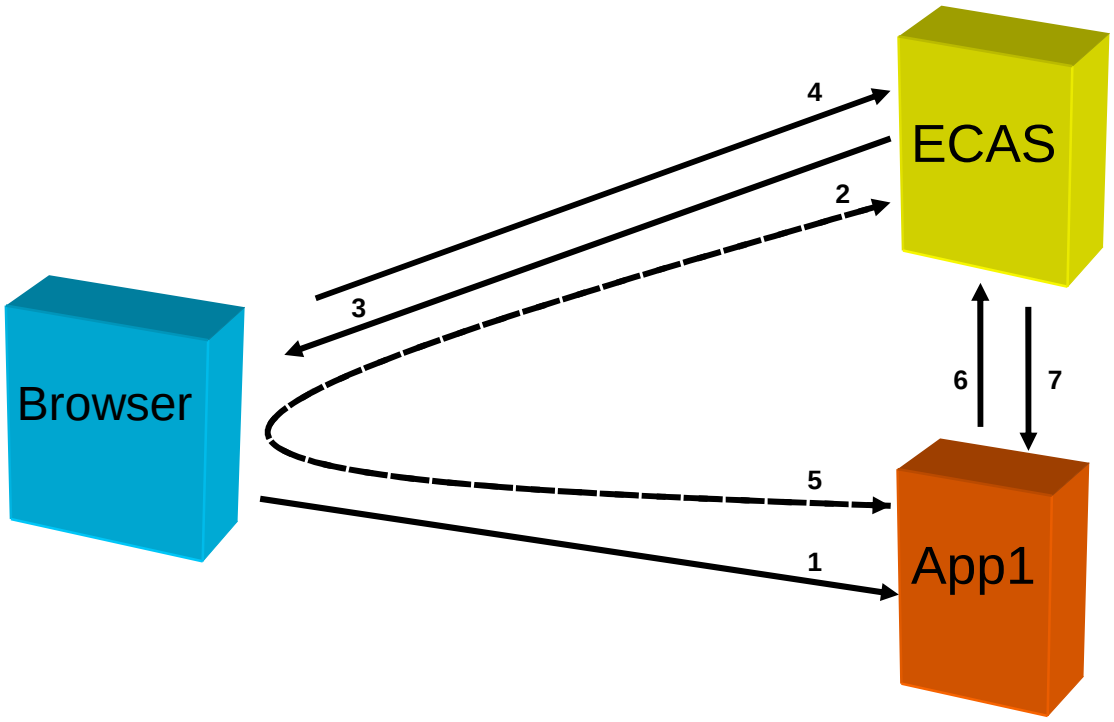
The purpose of ECAS is to provide a secure and common way for EC applications to authenticate their users and to simultaneously provide a single sign-on (SSO) to all applications that use it.

The service is available to any Commission system that needs to authenticate its users such as information systems or infrastructure components, otherwise referred to as ECAS client applications. ECAS clients are primarily web applications, but in the future, ECAS will also be available for other technologies.

ECAS allows applications to authorize users even though it does not actually perform any authorization, i.e. it does not determine whether or not an authenticated user has rights to access a certain resource. ECAS only uses passwords - always travelling on an encrypted channel - but it also provides support for stronger methods of authentication.

3.2 How does it work?

ECAS mechanisms work with simple HTTPS calls and redirections and do not rely on any specific technology such as strong encryption mechanisms.



A user making a first connection to an application (1) has no session established with the application, and so is redirected to ECAS (2) on a secure channel. The application specifies where the user must return after authentication.

ECAS presents a login/password screen (3) and the user enters his credentials (4). After successful authentication, ECAS redirects the call back to the application and adds a specific token, or ticket, to the request (5). At the same time, it sets an SSO cookie.

The application now receives a call from its user, along with a ticket number. The application validates the ticket by issuing a call to a specific ECAS URL (6) and ECAS answers by providing information about the user (7).

Based on the Yale University Open Source “CAS”, no user information is transmitted in an insecure way. Even if the application is called on HTTP, the ticket sent by ECAS contains no user information, and is valid only once. The actual user information is retrieved on the basis of the ticket on a secure channel.

The Single Sign On cookie that was set after successful authentication is a secure server (or application) session cookie: it is sent only to ECAS, always over HTTPS, and does not outlive the browser session (it is not stored physically on disk). This cookie is sent to ECAS when the user connects to a second application that requires authentication. Recognizing the cookie, ECAS does not present the login screen but instead redirects immediately to the application with a brand new ticket for the user.

Once the user has a session with the application, ECAS is no longer used: the requests are passed directly to the application.

3.3 Actors involved

End users comprise users of any system that is protected by ECAS. The first phase will only include internal users (Commission staff and contractors working on Commission premise) while in the second phase, certain groups of generic users (managed by service providers, usually external to the Commission) will also be able to be authenticated. The third phase will see generic users gradually replaced and supplemented by properly identified external users, managed by specific systems.

The ECAS service is managed by DIGIT.A.1; DIGIT.B.4 develops the ECAS software and, together with DIGIT.A.4, is also responsible for resolving problems relating to the internal functioning of the system.

In line with other operational services, the Service Centre handles all reports of incidents and problems. The system administrator monitors the proper technical functioning of the service and also maintains a list of client applications.

The Security Directorate defines the Commission’s authentication policy and is responsible for following up security incidents. It also conducts audits concerning the behaviour and the usage of the service.

4 Conclusions

Discussions with DG DIGIT and DG MARKT have shown that they are very interested in incorporating electronic identities into ECAS over the course of 2009 - especially for the purposes of the Internal Market Information System.

Although the finalisation of common specifications for EU eID interoperability through STORK require some time still, it might be recommendable, as a first step, to launch a pilot system including technical solutions for a limited number of Member States. Apparently, some ECAS tests have already been run on the Belgian citizen card.

The issue will be discussed again in the context of the STORK General Assembly in December, and by the beginning of 2009 a working group with technicians from the services involved will start to draft deliverable D7.4 "Common Specifications A2A", which is scheduled to be finalised in June 2009.

References

[1] IDABC Work Programme Fifth Revision (2008), Section I - Projects of common interest / Horizontal measures

[2] European Commission - ECAS local support guide (2005)