InterPARES Trust

Study Name:		Analysis of the Interoperability Possibilities of Implemented Governmental e-Services
Team & Study Number:		EU15
Research domain:		Control
Document Title:		Checklist
Status:		Final
Version:		v1.2
Date submitted:		20160727
Last reviewed:		
Author:		InterPARES Trust
Writer(s):		Hrvoje Stancic, Faculty of Humanities and Social Sciences, University of Zagreb Tomislav Ivanjko, Faculty of Humanities and Social Sciences, University of Zagreb Nikola Bonic, Ana Garic, Ksenija Loncaric, Ana Lovasic, Kristina Presecki, Ana Stankovic, GRAs, Faculty of Humanities and Social Sciences, University of Zagreb
Editor:		Corinne Rogers

Document Control

Version history			
Version	Date	By	Version notes
v 1.1	2016/07/27	Corinne Rogers	Adapted from EU15 Final Report
v 1.2	2016/07/28	Hrvoje Stancic	Minor revisions and improvements

Checklist for Single Sign-On Systems

This Checklist is designed to offer guidance to records managers and archivists in businesses, government agencies or other organizations to assess single sign-on (SSO) systems, as well as by SSO developers in order to ensure that they have provided sufficient information on the system they are developing in order to detect the possibilities of exchanging identification and authentication credentials.

It is the result of a study in the international InterPARES Trust Research Project (https://interparestrust.org), EU15: Analysis of the Interoperability Possibilities of Implemented Governmental e-Services in the EU, which investigated the differences in the level of development of e-Services with a focus on aspects important for their implementation as *trusted* e-Services. The study analyzed the implemented governmental e-Services in the EU in the context of national single sign-on systems in order to detect possibilities of exchanging identification and authentication credentials among them thus creating a network of trust between the national systems enabling citizens to seamlessly use other country's e-Services. Single sign-on systems and their key components were analyzed in 28 European countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. EU15 built on the findings of EU09: Comparative Analysis of Implemented Governmental e-Services, which found that there was an absence of publically available information important for establishing trust in e-Services, particularly information about 'Storage and long-term content availability' and 'System operation transparency.'[1]

The checklist is based on the questionnaire used during the collection of data for analysis of single sign-on systems and their key components implemented in the EU, as a part of e-government initiatives, and slightly improved. The research team believes that this checklist provides sufficient information to assess the possibilities of exchanging identification and authentication credentials.

The checklist consists of 19 questions divided into 5 categories as following:

1. Legal Framework and Strategies (1 question),
2. Portals (1 question),
3. Single Sign-on (SSO) (11 questions),
4. Trust mechanisms – technical details (5 questions),
5. Future plans (1 question).

[1] See the EU09 final report, available at https://interparestrust.org/assets/public/dissemination/EU09_20160727_ComparativeAnalysisGovernmentaleServices_FinalReport.pdf.

Checklist for Single Sign-On Systems

	Question	Y	N	?[2]	Additional info[3]
1. Legal Framework and Strategies					
1.	Is there a national IT strategy concerning e-Government?				
2. Portals					
2.	Is there a central e-Government portal?				
3. Single Sign-on (SSO)					
3.	Is there a SSO system in place?				
4.	Is the system implemented after 2010?				
5.	How are users authenticated?				
	Username/password				
	e-Certificate				
	eID card				
	e-Signature				
	m-token/mobile ID				
	PIN				
	Single-use code				
	Smart Card				
	Token				
	Other				[Add method]
6.	Is there a physical aspect involved in e-Identification (token, smart card, SIM card ...)?				
7.	Are there one or more levels of access depending on different user's credentials?				
8.	Is there a central identity data governing body? (Central Directory/Register?)				
9.	What is the source of users' identity for obtaining user authentication?				
	Social Security Number (SSN)				
	Driver's license				
	ID				
	Passport				
	Other				[Add method]
10.	Are there different terms of use for domestic and foreign users?				

[2] The "?" column indicates a situation where no information is available or the question is not applicable to your situation.

[3] The "Additional info" column can be used in situations where a simple "Yes" or "No" answer can be supplemented with useful info, e.g. the web address of a central e-government portal, or a link where additional info on the matter in question can be found.

11.	Which services are connected via SSO?				
	Income taxes: declaration, notification of assessment				
	Job search services by labor offices				
	Social security benefits				
	Personal documents: passport and driver's license				
	Car registration (new, used, imported cars)				
	Application for building permission				
	Declaration to the police (e.g. in case of theft)				
	Public libraries (availability of catalogues, search tools)				
	Certificates (birth and marriage): request and delivery				
	Enrolment in higher education/university				
	Announcement of moving (change of address)				
	Health related services (interactive advice on the availability of services in different hospitals; appointments for hospitals)				
12.	Is there a possibility of log-on to a connected service without using SSO, i.e. by accessing their web-site directly and using their log-on service (different credentials from SSO credentials)?				
13.	Is it possible to obtain an e-document from one e-service and send it to another e-service via safe transfer methods – safe document transfer?				
4. Trust mechanisms – technical details					
14.	Does the system have single sign-off implemented, i.e. when user logs off from one service, does the system automatically logs off the user from all services he/she accessed during that session?				
15.	Are there some federated authentication standards supported and used (e.g. SAML)				
16.	Does the system require digital signatures? If yes – which type(s) – standard or advanced, XMLDSig, XAdES etc.?				
17.	Is it possible to achieve protocol interoperability (LDAP)?				
18.	Is the SSO a part of STORK initiative?				
5. Future plans					
19.	Are there any plans in place for future Identity Federation solutions				