LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dottorato di Ricerca in Sistemi Informativi Aziendali - XXI ciclo

Fiducia e tecnologia nelle relazioni elettroniche inter-organizzative

Candidato:
Dott. Stefano Za

Relatore:
Chiarissimo Prof. Alessandro D'Atri

Dipartimento di Scienze Economiche e Aziendali

Indice generale

INTRODUZIONE

1. La fiducia e le relazioni

Le relazioni tra individui o organizzazioni hanno sempre avuto ruolo rilevante nel contesto privato, sociale ed economico. Ultimamente tale ruolo è divenuto di notevole importanza, dato che persone e/o organizzazioni spesso per raggiungere i propri obiettivi, si trovano a dover creare, sviluppare o mantenere relazioni. Generalmente, ci sono diverse componenti che influenzano (positivamente o negativamente) una relazione; una tra le più importanti è la fiducia. Per alcuni, come Chiles and McMackin (1996), la fiducia è un fattore chiave in una relazione.

In letteratura sono presenti diversi studi che danno una definizione di fiducia o presentano una review al fine di trovare o fornire una definizione comune che tenga conto di diversi aspetti: sociale, organizzativo, psicologico o anche informatico (Rousseau et al. 1998; McKnight and Chervany 2001, Kramer 1999, Mayer et al. 1995).

Margaret Levi (1996) ha scritto: “La fiducia non è una singola cosa e non ha una sola sorgente; essa ha varietà di forme e cause” ("Trust is not one thing and it does not have one source; it has a variety of forms and causes"). Alcuni autori considerano la fiducia come risultato della combinazione di credenze, atteggiamenti, intenzioni e comportamenti (Bhattacherjee 2002), mentre altri vedono la fiducia strettamente legata alla valutazione del rischio (Mayer et al. 1995).

Da un punto di vista organizzativo, la fiducia è fortemente legata al concetto di comportamento opportunistico (Chiles and McMackin 1996). Se vi è un'alta

percezione del livello di fiducia, le parti saranno molto probabilmente spinte ad adottare regole meno elaborate per proteggere i propri interessi, il contrario avverrebbe se la percezione del grado di fiducia fosse molto bassa. Se si considerano la teoria dei costi di transazione (Williamson 1985) e l'agency theory (Eisenhardt K. 1985), i costi, in entrambi i casi (transaction costs e agency costs), sono spesso legati al controllo e limitazione di potenziali comportamenti opportunistici dei partner.

Fiducia e comportamenti opportunistici nella Transaction Cost Theory

Da un punto di vista dei costi di transazione, si può notare come il concetto di fiducia o di comportamenti opportunistici (per evitare e/o controllare) è presente nelle quattro fasi (Ciborra 1989) che li caratterizzano :

- ricerca: costituzione della coppia di contraenti (avviamento) – *percezione del grado di fiducia nel potenziale partner*;
- contrattazione: redazione del contratto e investimenti specifici (*investimenti per la creazione del clima di fiducia*);
- controllo e regolazione: esecuzione del contratto e vigilanza (*evitare comportamenti opportunistici*);
- mantenimento: investimenti specifici (necessità di percezione di equità durante la transazione – *controllo*)

Fiducia e comportamenti opportunistici nell'Agency Theory

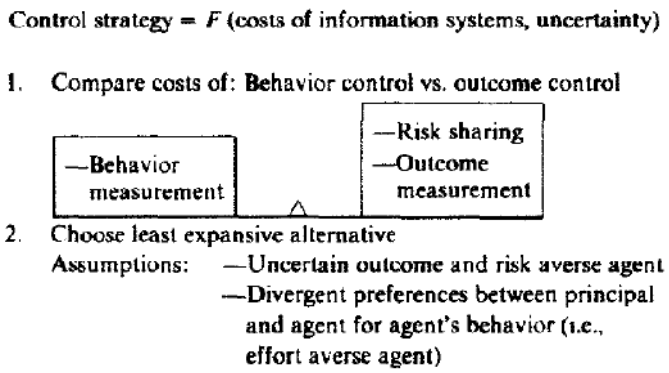

Figura 1. *The Agency Theory (Eisenhardt K. 1985)*

Da un punto di vista relazionale, utilizzando come definizione di "agency relationship" quella di Jensen and Meckling (1976), la si può vedere come un contratto sotto cui uno o più individui (o organizzazioni – the principal(s)) ingaggiano una terza persona (the agent) per eseguire alcuni servizi per loro conto, delegandogli un certo grado di autorità nelle decisioni.

Se entrambi le parti della relazione sono portate a massimizzare le utilità derivanti da essa, è facile pensare che l'agent non sempre agirà nel migliore dei modi per gli interessi del principal(s).

Gli "agency cost" sono quei costi sostenuti o per il controllo o per la protezione contro potenziali comportamenti opportunistici dell'agent (società o singolo).

Pertanto, l'approccio alla gestione dei costi (agency cost) è teso a controllare da vicino l'altra parte (l'agente), o a usare contratti, incentivi, penalizzazioni, tecnologia per controllare e garantire la conformità del loro operato al contratto. In ultima analisi, se si opta per l'integrazione dell'agente nella gerarchia organizzativa, in modo da ottenere il pieno controllo ed allineamento del comportamento dell'agente con gli

interessi della società, anche in questo caso, bisogna prevedere investimenti per progettare e realizzare strumenti necessari per il controllo.

Una tassonomia delle relazioni

A causa della sempre più alta pervasività tecnologica, favorita dalla diffusione dell'uso di internet, possiamo distinguere due tipi principali di relazioni in base a cui si individuano i concetti di fiducia:

1. Tradizionale: relazioni in cui l'IT gioca un ruolo marginale. In questo caso si individuano due concetti principali di fiducia: istituzionale (McKnight, 1998) e sociale (spesso definita come "customer trust") (Granovetter, 1985).
2. Digitale (o online): relazioni completamente basate su IT. In questo contesto (E-business/E-service/E-commerce/e-Marketplace) l'IT influenza il concetto di fiducia sia istituzionale sia sociale; oltre a questi due concetti bisogna considerarne anche un terzo: la fiducia nella tecnologia (Reeves and Nash 1996, Misiolek et al. 2002, Ratnasingam and Pavlou, 2002).

Questo lavoro partirà dal considerare le relazioni del secondo tipo, proponendo, sulla base del TFI model, un modello concettuale con cui vedere le tre tipologie di fiducia che le caratterizzano. Successivamente si considererà solo il concetto di fiducia nella tecnologia e si fornirà una tassonomia dei meccanismi tecnologici, fatta in base alle funzionalità fornite, composta da tre classi. Da qui, considerando solo la prima delle tre, si presenterà un analisi di due casi in cui si descrivono i risvolti (effettivi e potenziali) scaturiti dall'adozione di un particolare sistema tecnologico.

2. Framework teorico

In questo paragrafo si presenta il modello TFI (technical, formal and informal model) (Stamper et al 2000) che verrà utilizzato successivamente come lente per analizzare il ruolo della fiducia nelle relazioni elettroniche, proponendo un modello concettuale.

Modello TFI – tecnico, formale ed informale.

Per comprendere meglio quanto descritto sin ora, relativamente al concetto di relazione, si fornisce un punto di vista composto da tre livelli che si influenzano di continuo e vicendevolmente (Liebenau and Backhouse 1990): tecnologico, formale e informale. In questo framework concettuale basato sulla semiotic theory, i modi informali di gestire le informazioni sono critici e non possono sempre essere sostituiti da regole o vincoli imposti dal sistema tecnologico.

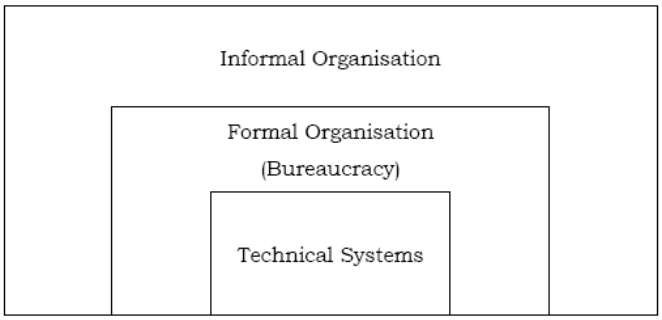

Figura 2. *The embedding of computer systems in the formal and informal organisation (Stamper et al, 2000)*

In questa prospettiva, gli elementi informali (vale a dire la percezione del rischio, le credenze, la cultura, ecc.) strettamente legati al contesto, guidano la progettazione e la selezione di elementi formali (politiche, processi aziendali, norme, procedure, ecc)

e soluzioni tecnologiche (piattaforme hardware e software, infrastrutture di rete, dispositivi, ecc.).

Nel contesto dei sistemi informativi, in particolare nel campo delle relazioni elettroniche, il rapporto tra questi tre livelli è oggi più complesso e richiede di affrontare altre questioni (fiducia, privacy...) per mezzo di meccanismi tecnologici, formali e informali che possono essere riassunte come segue (Gambetta 1998, Kumar et al. 2007):

1. la percezione di sicurezza incorporato nel sistema tecnologico (livello informale);
2. la presenza di meccanismi formali che regolano le interazioni (livello formale);
3. l'affidabilità dei sistemi ICT (livello tecnologico).

Partendo da questo modello, si può guardare la relazione come composta da elementi basati su i tre livelli: informale, formale e tecnologico.

Modello concettuale

Come nelle relazioni tradizionali, la fiducia è considerata cruciale nelle relazioni elettroniche (Ba et al. 1999). Dato che internet è considerato un ambiente "non sicuro" (Ratnasingam 2002), l'IT influenza fortemente il livello di fiducia (Misiolek et al. 2002):

1. Social trust: fortemente legata alla percezione del rischio nello scambio di informazioni tra le parte (Koller 1988), influenzata principalmente da esperienze positive;

2. Organizational trust (institutional trust): relativa alle relazioni tra individui (organizzazioni se gli individui ricoprono il ruolo di decisori) e organizzazioni supportate dall'information technology (Lewicki & Bunker, 1996; Tyler & Degoey, 1996, Pavlou et al. 2003, Spagnoletti et al. 2007, McKnight et al. 1998)
3. Technological trust: relativo al rapporto con l'IT usato a supporto per lo scambio delle informazioni (Reeves and Nash 1996), anche definita come la probabilità con cui le organizzazioni credono che l'infrastruttura tecnologica sottostante è in grado di facilitare le transazioni compatibilmente con le loro aspettative (Ratnasingam e Pavlou, 2002).

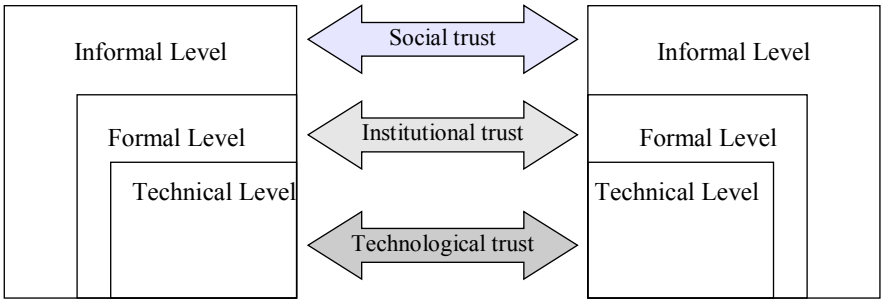

Figura 3. *The relationships between the three trust concepts and the TFI levels*

Volendo analizzare le relazioni tra individui (quali decisori all'interno di un'organizzazione) ed organizzazioni, si utilizza il modello TFI presentato precedentemente, per analizzare la tipologia di fiducia coinvolta ad ogni livello.

Lo schema riportato in figura 3 illustra la relazione tra individuo ed organizzazione scomposta nei tre livelli.

Se la percezione del livello di fiducia sociale (o personale, basata tendenzialmente su esperienze positive) è alta, la relazione coinvolge principalmente il livello informale, ed è quindi regolata da modi di operare e consuetudini ormai consolidate (influenzate

per esempio anche da culture e modi di vivere comuni). Se così non fosse, a livello formale verrebbero adottate maggiormente regole e norme per governare le relazioni, contribuendo così all'aumentare del livello di fiducia istituzionale. Se le regole formali non sono sufficienti per avere un adeguato livello di fiducia tale da permettere la relazione, vengono introdotti meccanismi tecnologici a supporto, interessando così il concetto di fiducia tecnologica. In tal modo, le regole formali e i meccanismi tecnologici vengono coinvolti in sequenza in base al livello più o meno basso di fiducia sociale, mirando principalmente a diminuire la probabilità di (o di limitare) comportamenti

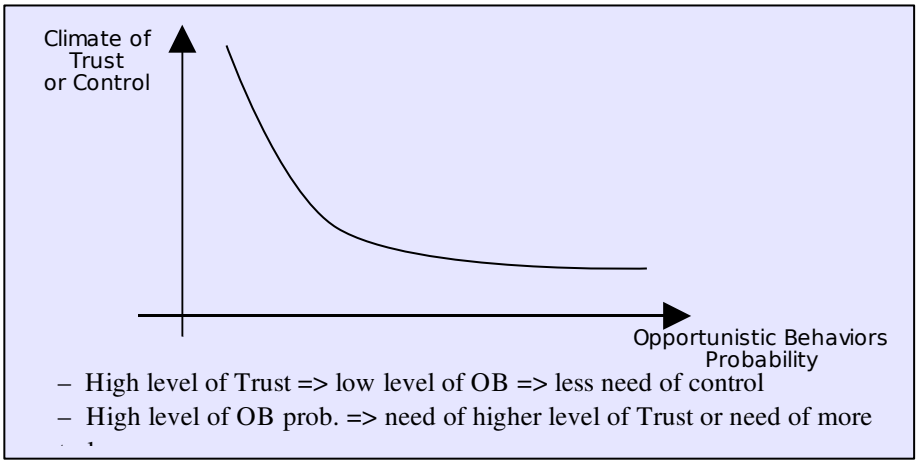

Figura 4. *Trust and control vs Opportunistic Behaviours*

opportunistici da parte del partner. È questo lo scenario tipico delle relazioni basate completamente sull'IT (vedi figura 4).

Volendosi concentrare sul concetto di fiducia tecnologica, in questo lavoro non si considerano quei fattori (tecnologici e non) che influenzano direttamente la fiducia sociale o istituzionale (per esempio i meccanismi di feedback che mirano ad aumentare la reputazione del soggetti a cui fanno riferimento) nel contesto

elettronico; ma piuttosto si mira a quei meccanismi che agiscono direttamente sul livello di fiducia nella tecnologia utilizzata a supporto della relazione.

Relativamente a questo ultimo punto, essendo questo tipo di relazioni basate principalmente sulla gestione e trasferimento di informazioni, le funzionalità tecnologiche che influenzano maggiormente il livello di fiducia sono quelle legate ai meccanismi di sicurezza. Questo lavoro partendo sulla classificazione dei sette meccanismi IT definita da Ratnasingam (2002), propone una tassonomia alternativa strutturata in classi che identificano tre principali tipologie:

1. accesso alle informazioni (o risorse): legate ai concetti di autenticazione, identificazione, autorizzazione
2. trasferimento delle informazioni: legate alle tipologie e mezzi utilizzati (protocolli, tipo di trasmissione) – confidenzialità ed integrità
3. gestione delle informazioni: legate alle policy adottate per assicurare la disponibilità delle informazioni e per far fronte a potenziali perdite impreviste dei dati (fault tolerance, backup, copie dei dati delocalizzate, etc.) – disponibilità

Tale classificazione parte dal presupposto che le relazioni elettroniche basate completamente su l'IT siano strutturate in tre fasi principali: l'accesso alle informazioni (in cui viene presentata la richiesta e validata), il trasferimento delle informazioni (una volta validata la richiesta, esse vengono trasmesse utilizzando una serie di mezzi e policy per garantirne la confidenzialità e l'integrità), la gestione delle informazioni (focalizzata sul garantire la loro disponibilità, necessaria per adempiere alle richieste valide). Di seguito viene fornita la classificazione di Ratnasingam (Figura 5) che successivamente verrà confrontata con quella fornita in questo lavoro.

Technology trust mechanisms and their relationship with Web services

Technology trust mechanisms	Relationship to Web services
Confidentiality mechanisms refer to the protection of transactions sent and received via Web services against unauthorized reading, copying, or disclosure using encryption mechanisms	Web services use encryption, user IDs and passwords to maintain the confidentiality of the transactions and messages exchanged between the requesters, providers, and brokers on the Web
Authentication mechanisms provide transaction quality of being authoritative, valid, true, genuine, and worthy of acceptance or belief by reason of conformity to the fact that reality is present in Web services	Web services apply the standard authentication protocol (HTTP) along with SSL as a customary choice, although over time large corporations using Web services for sensitive information and financial transactions move to digital certificates
Integrity mechanisms refer to transaction accuracy and assurance that Web services transactions have not been altered or deleted	Web services use reliable messaging to enforce integrity ensuring that the message was only sent once, thus avoiding duplicate messages (Snell, 2001). In addition dependency spheres a new type of transaction context that allows both synchronous and asynchronous distributed messaging style exchanges to occur within a single transaction
Non-repudiation mechanisms protect providers, requesters, and brokers in Web services via acknowledgement procedures	Web services use reliable messaging to ensure that both the provider and requester of a service know whether or not a message was actually sent
Availability mechanisms protect Web services transactions against weaknesses in the transmission media	Web services have features that enable the logging, configuration, and deployment of utilities via Web access
Access controls mechanisms provide authorization mechanisms thereby assuring that Web services transactions are sent and received without interruption	Web services use conditional messaging to establish various conditions that apply to how and when a message was delivered. For example, a price quote for 10,000 Think Pad laptops may only be valid for 10 days after the quote has been received. Conditional messages are based on rules implemented on the application layer (top layer). Conditional messaging allows companies to dynamically integrate their business processes within defined constraints and conditions
Best business practices focus on policies, procedures, standards, and top management commitment that enforce regular audit, and ensure the smooth functioning of Web services	Web services use open standards such as XML, SOAP, UDDI and WSDL that facilitate Web services to be described, advertised, discovered, and involved on the Internet. These open standards enable an infrastructure for Web services to function across multiple platforms. SOAP provides the basic program to program glue that enables applications to bind together. UDDI provides the full repository lookup

Figura 5. *Ratnasingam's seven mechanisms of technology trust*

Nella tabella seguente vengono messi a confronto i 7 meccanismi abilitanti il “trust technology” (confidenzialità, autenticazione, integrità, non-ripudio, disponibilità, controllo degli accessi, best business practices) e la classificazione fornita in questo lavoro, al fine di evidenziare la corrispondenza tra le due tassonomie.

Tassonomia proposta	**Ratnasingam's mechanisms**
1. Accesso alle informazioni	*2. Autenticazione, 6. Controllo degli accessi,*
2. Trasferimento delle informazioni	*1. Confidenzialità, 3. integrità, 4. non-ripudio,*
3. Gestione delle informazioni	*5. disponibilità,*
Trasversale (non rientra esclusivamente in una delle tre classi)	*7. Best business practices (trasversale, può incidere anche direttamente sulla fiducia a livello più alto)*

Tabella 1. *Centralized vs federated system*

Una volta identificate queste tre classi, si è presa in considerazione la prima, nella quale rientrano le infrastrutture per la gestione delle autenticazioni e autorizzazioni (d'ora in avanti AAI).

Nel prossimo paragrafo si descriverà il concetto di AAI ed il loro impiego nel contesto delle relazioni inter-organizzative.

3. Sistemi per la gestione delle autenticazioni e autorizzazioni: le AAI (authentication authorization infrastructure)

Nel contesto elettronico, due o più organizzazioni decidono di collaborare per una determinata opportunità di business o anche per necessità. In entrambi i casi si instaurano delle relazioni tra i partner. In genere, nel contesto di riferimento, le relazioni riguardano il trasferimento di informazioni supportato dal fatto che ognuna di esse fornisce uno o più servizi alle altre componenti, ricoprendo spesso il ruolo sia di fruitore sia di erogatore di servizi. Questi ultimi verranno utilizzati dai dipendenti (o dai clienti a seconda dello scenario) di ogni partner in base alla tipologia del servizio e alle policy scelte. Tale accesso tendenzialmente potrà essere fatto solo dopo un processo di autenticazione sul quale si baserà quello di autorizzazione.

E' il caso ad esempio di filiere di organizzazioni che erogano servizi in contesti delocalizzati e secondo modalità fortemente basate sulle tecnologie ICT. In tale ambito assumono importanza, nel determinare il livello di fiducia percepita dalle parti (percezione del clima di fiducia durante le transazioni (Ciborra, 1989)), le modalità con cui si gestiscono e scambiano le informazioni.

In questo contesto, particolare importanza ricoprono i sistemi di autenticazione e autorizzazione (AAI) all'interno di un network di imprese, dove ogni impresa può ricoprire il ruolo di fornitore e/o richiedente di uno o più servizi. In questo ultimo caso sarà tale impresa a dover gestire le informazioni legate alle identità dei richiedenti (siano essi propri clienti o propri dipendenti) nella richiesta del servizio verso terzi.

In questo scenario, coloro che richiedono il servizio riporranno maggiore o minore fiducia nell'azienda erogatrice in base a diversi aspetti legati alla gestione delle proprie informazioni.

Da un punto di vista tecnologico le procedure che determinano o meno l'accesso ad un determinato insieme di servizi e/o informazioni sono supportate da una AAI, la quale si occuperà di verificare le credenziali di accesso (es.: username e password) e le relative autorizzazioni (chi può fare cosa).

Attualmente esistono due principali tipologie di AAI: il sistema centralizzato e il sistema federato.

Si propone di seguito un'analisi dei vantaggi e degli svantaggi, nell'adottare uno o l'altro, da un punto di vista della fiducia relativamente alla gestione delle informazioni.

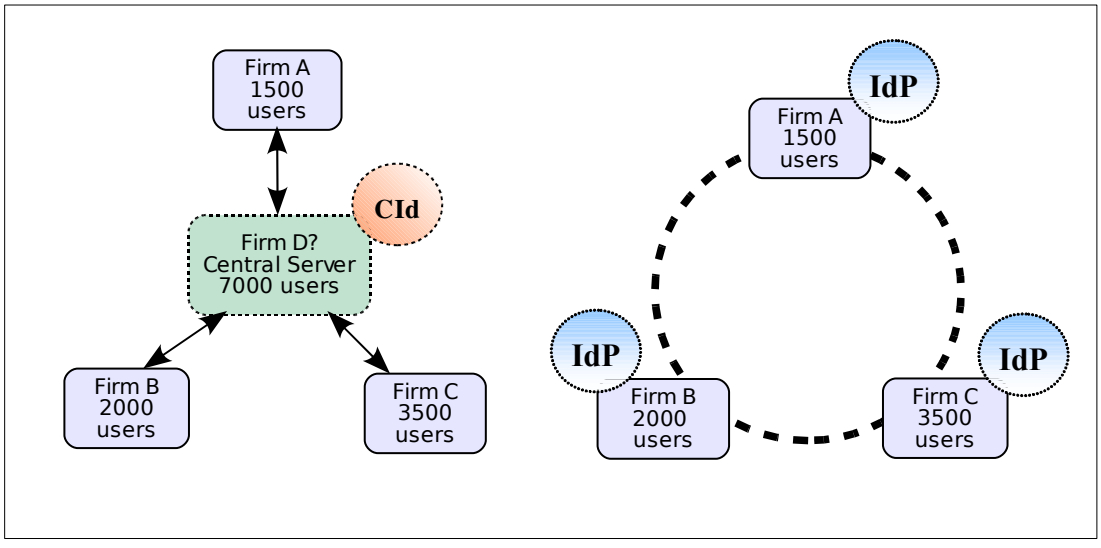

Figura 6. *AAI: centralized system vs federated system*

	Centralizzato	Federato
Chi e come sono gestite le identità	**Uno dei partner o un terzo:** *necessità di creare clima di fiducia*	**Ognuno gestisce le informazioni degli utenti di propria competenza**
Altri fattori che possono favorire le relazioni		
Problemi di sincronizzazione	Presenti	Non presenti
Possibilità di far parte di più network	Procedimento complesso, generalmente non previsto	Rientra nelle caratteristiche del sistema

Tabella 2. *Centralized vs federated system*

Se il gruppo adottasse un sistema centralizzato per controllare l'accesso a uno o più servizi, si dovrà decidere chi svolgerà il ruolo di Central Identity provider (CIdP), in cui risiederanno tutte le informazioni legate alle identità degli utenti (dipendenti o clienti) di tutti i partner coinvolti.

Gli scenari possibili sono sostanzialmente due, in cui il CIdP è uno dei partner oppure lo è un'organizzazione esterna, probabilmente specializzata in questo tipo di attività (nella quale si riconosce notevole grado di fiducia istituzionale). In entrambi i casi è necessario creare un clima di fiducia tra il fiduciario (chi gestisce le informazioni relative alle identità) e ed ogni partner (società che utilizza il servizio).

Lo scenario si complica ulteriormente se una o più società sono partner in più di un gruppo (o network).

Se la scelta cadesse su un sistema di tipo federato invece, ogni organizzazione gestirebbe le informazioni legate alle identità dei propri utenti per proprio conto, non avendo così la necessità di creare un alto clima di fiducia tra le parti. Tale gruppo di organizzazioni è definito circolo di fiducia (circle of trust) in cui ogni partecipante può agire sia da Service Provider e/o da Identity Provider. Inoltre ognuno di essi può unirsi facilmente a diversi gruppi mantenendo al proprio interno la gestione delle informazioni sensibili legate alle identità degli utenti..

I sistemi federati per la gestione delle Autenticazioni e Autorizzazioni

Per meglio comprendere questo tipo di architettura, conviene introdurre il concetto di "Circolo di Fiducia", utilizzato diffusamente nella documentazione di uno dei principali progetti per la definizione di standard e specifiche che implementano sistemi federati di gestione delle identità[1]. Un Circolo di Fiducia (circe of trust, anche noto come federazione), è definito come un gruppo di organizzazioni che hanno stabilito degli accordi sulle modalità di interazione nella gestione delle identità degli utenti. Una volta che un utente effettua l'autenticazione presso un Identity Provider (IdP) appartenente ad un Circolo di Fiducia, lo stesso utente può usufruire dei servizi forniti da qualsiasi Service Provider (SP) appartenente allo stesso Circolo. Tra le specifiche del progetto Liberty, sono descritti alcuni meccanismi per fornire funzionalità di single sign-on e per collegare account separati entro un gruppo di Service Provider appartenenti ad un Circolo di Fiducia.

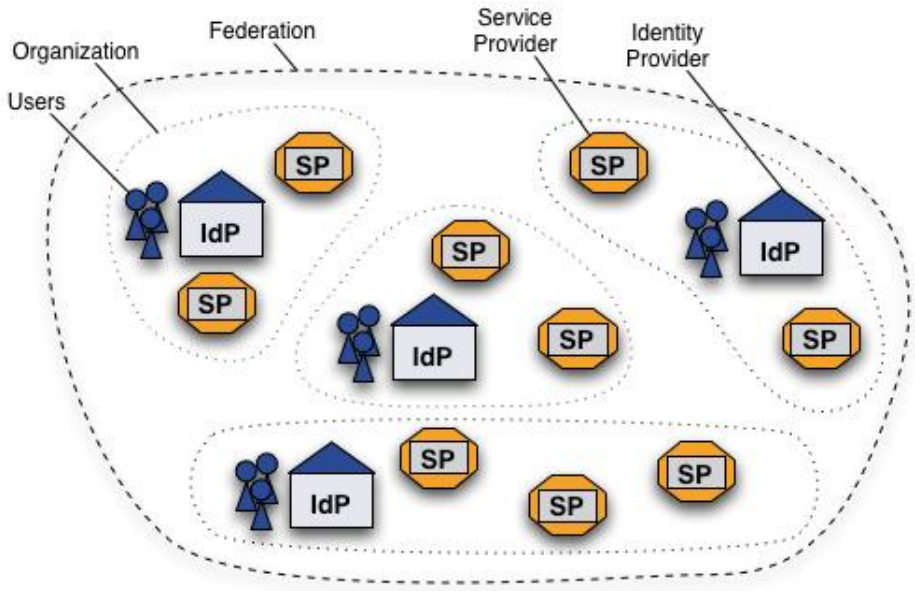

Figura 7. *Circle of Trust.*

[1] Si tratta del progetto Lyberty Alliance (www.prejectliberty.org)

Nell'architettura federata proposta sono presenti tre principali tipi di soggetti. Con il termine soggetto, in questo caso, si fa riferimento a:

1. Identity provider (IdP – nel quale risiedono i dati di registrazione degli utenti)

2. Service Provider (SP – fornisce uno o più servizi)

3. User agent (UA - l'applicazione dell'utente che comunica con l'IdP o con il SP)

A livello tecnologico, l'interazione tra i soggetti avviene mediante Web services (comunicazione tra IdP e SP), Web redirection (l'IdP ed il SP comunicano indirettamente attraverso lo UA), Schemi e Metadati (utilizzati nella comunicazione tra SP ed IdP).

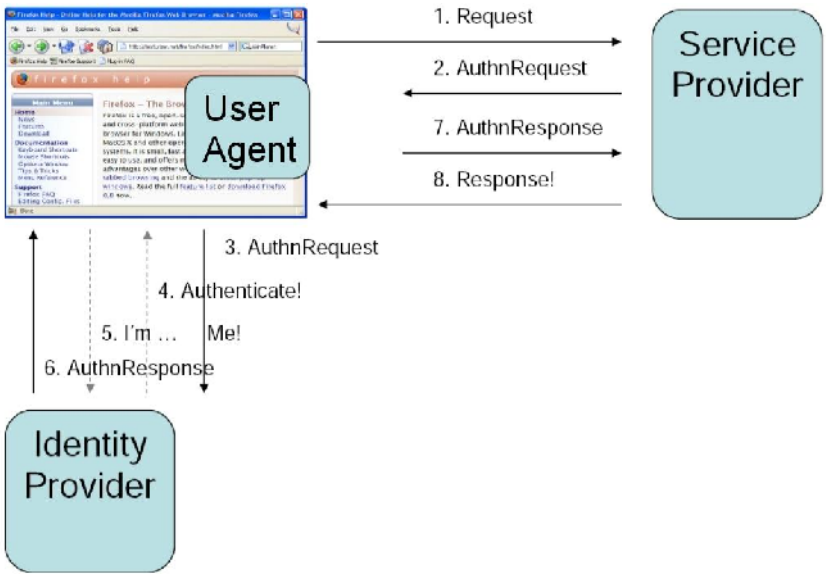

Figura 8. *Authentication process*

Nel momento in cui un utente accede al Circolo, il suo IdP crea un "handle" e lo invia al suo user agent. Tale handle è affidato allo user agent fino al momento del logout ed è accettato da qualsiasi IdP o SP appartenente al Circolo di Fiducia. Ogni volta l'utente tenta di accedere ad uno dei Service Provider, il suo handle passa a

quest'ultimo che lo utilizza per richiedere le credenziali dell'utente all'Identity Provider di appartenenza (senza ulteriori interventi da parte dell'utente). Infine, quando l'utente effettua il logout, il suo Identity Provider si occupa di inoltrare un messaggio a tutti gli altri Service Provider e memorizza l'handle per evitare che lo stesso sia riutilizzato in futuro. I meccanismi finora descritti consentono dunque all'utente di eseguire l'accesso una sola volta durante ciascuna sessione (Single Sign On) e di interagire con ciascuno dei Service Provider all'interno del Circolo di Fiducia.

In una tale configurazione, ciascuno dei Service Provider rappresenterebbe un possibile punto d'accesso per l'utente e la fiducia istituzionale tra i membri dell'organizzazione sarebbe favorita dagli accordi formali previsti dal Circolo di Fiducia. Inoltre i dati personali di registrazione sarebbero conservati dal solo Identity Provider, con implicazioni sugli aspetti relativi alla privacy.

4. Domanda di ricerca e struttura della tesi

Dopo aver presentato in questo capitolo il modello di analisi, all'interno della tesi verranno descritti due casi di adozione di un sistema federato come meccanismo per favorire il clima di fiducia tra le parti. Utilizzando l'approccio interpretativo della design research si descriveranno i possibili benefici derivanti.

Proponendo lo schema di Hevner (Hevner et al. 2004 – figura 9), questo lavoro ha presentato in questo capitolo un modello concettuale per analizzare il ruolo della fiducia nelle relazioni elettroniche inter-organizzative, utilizzando come lente il modello TFI; successivamente si analizzerà l'adozione di un particolare meccanismo tecnologico (artifact) su due casi.

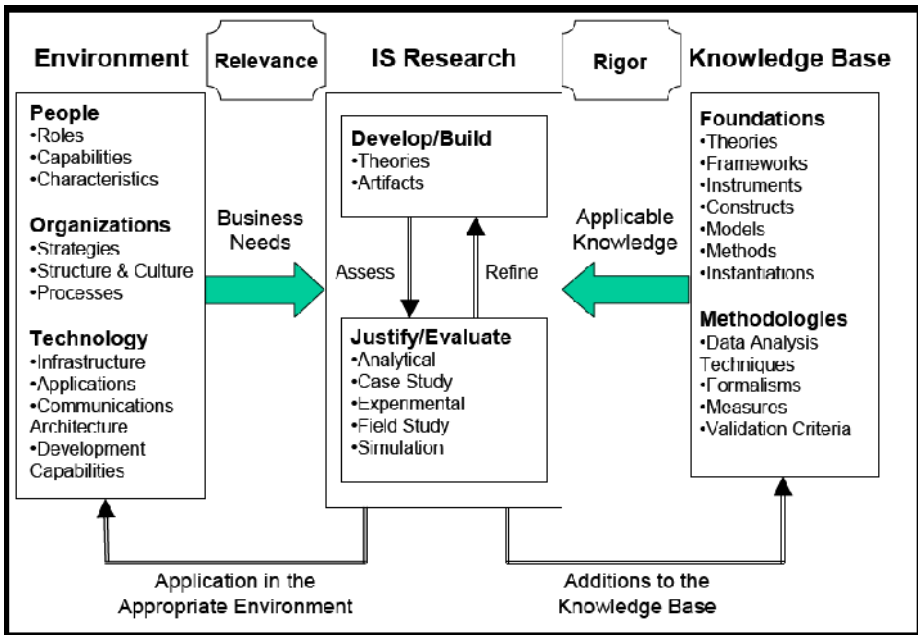

Figura 9. *Information Systems Research Framework (Hevner et al. 2004)*

Il primo caso è puramente concettuale ed analizza la struttura organizzativa delle virtual organization; propone l'adozione di questo tipo di sistema come facilitatore nelle relazioni tra i soggetti dell'organizzazione virtuale (partendo dal modello ECB – Enabler, Catalyst, Enabler) e relativi utenti. I contenuti di questo capitolo si basano sull'articolo presentato al "VIII Workshop Docenti e Ricercatori di Organizzazione Aziendale" (Spagnoletti e Za, 2007).

Il secondo caso descrive l'adozione del sistema federato all'interno di un progetto europeo (LD-CAST[2]) che mira alla cooperazione delle camere di commercio dei paesi coinvolti (Romania, Polonia, Bulgaria, Italia) al fine di fornire agli imprenditori

[2] Il progetto LD-CAST (Local Development Cooperation Action Enabled by Semantic Technology) è stato fondato dalla Commissione Europea, all'interno del sesto programma quadro di Ricerca e Sviluppo. Lo scopo del progetto è di sviluppare reti integrate Europee per l'erogazione di servizi pubblici interoperabili rivolti alle piccole e medie imprese.

delle nazioni partner un servizio integrato relativo all'avvio di attività trans-nazionali (Spagnoletti e Za, 2008).

Successivamente verrà proposta un analisi di 25 casi nei quattro contesti di maggiore adozione di questo sistema (sulla base della reportistica presente sul sito del progetto Liberty Alliance[3]) identificando quali sono le motivazioni maggiori, relativamente al contesto, che portano all'utilizzo di questo sistema (Za, 2007).

[3] http://www.projectliberty.org/

5. Bibliografia

Åhlfeldt R.M., Spagnoletti P. and Sindre G. (2007). Improving the Information Security Model by using TFI", 22nd International Information Security Conference, IFIP SEC 2007 Conference, 14-16 May 2007, Sandton, Gauteng, South Africa

Ba, S., Whinston, A. B., and Zhang, H. (1999). Building trust in the electronic market through an economic incentive mechanism. In Proceedings of the 20th international Conference on information Systems (Charlotte, North Carolina, United States, December 12 - 15, 1999). International Conference on Information Systems. Association for Information Systems, Atlanta, GA, 208-213.

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. Journal of Management Information Systems, 19 (1), 211-242.

Ciborra C. (1989) "Tecnologie di Coordinamento" Franco Angeli, Milano, 142-145

Chiles, T.H. and McMackin, J. (1996). Integrating variable risk preferences, trust, and transaction cost economics, Academy of Management Review 21 73–99.

Eisenhardt K. (1985). Control: organizational and economic approaches. Management Science, 31, 134-149

Erber, R., Schläger, C., Pernul, G. (2007) Patterns for Authentication and Authorisation Infrastructures. Proc. of the 1st International Workshop on Secure Systems Methodologies using Patterns (SPattern'07), Regensburg, Germany.

Fernandez, E. B., Pernul, G., Larrando-Petrie, M. (2008). Patterns und Pattern Diagrams for Access Control. Proc. of the 5th International Conference on Trust, Privacy & Security in Digital Business (TrustBus '08), Italy.

Gambetta, D., (1988). Trust: Making and Breaking Cooperative Relations. Basil Blackwell, Oxford, U.K. ed. 1998

Granovetter M. (1985), "Economic Action and Social Structure: The Problem of Embeddedness." American Journal of Sociology, 91(November): 481-510.

Gunetti, D., Picardi, C. (2005). Keystroke analysis of free text, ACM Trasactions On Information and System Security, 3(5), 312-347.

Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004) "Design Science in Information System Research," MIS Quarterly, 28:1, pp. 75--105.

Jensen M. C. and Meckling W. H., Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure(July 1, 1976). Michael C. Jensen, A THEORY OF THE FIRM: GOVERNANCE, RESIDUAL CLAIMS AND ORGANIZATIONAL FORMS, Harvard University Press, December 2000; Journal of Financial Economics (JFE), Vol. 3, No. 4, 1976.

Koller, M. (1988). "Risk as a Determinant of Trust," Basic and Applied Social Psychology Volume 9, Issue 4, pp. 265-276.

Kramer R. M., (1999), “Trust and distrust in organizations: Emerging Perspectives, Enduring Questions”, Annual Review of Psychology, Vol. 50: 569 -598.

Kumar, K. and Becerra-Fernandez, I. (2007). Interaction technology: Speech act based information technology support for building collaborative relationships and trust. Decis. Support Syst. 43, 2 584-606. DOI= http://dx.doi.org/10.1016/j.dss.2005.05.017

Levi, M. (1996). Social and unsocial capital: a review essay of Robert Putnam's "Making Democracy Work". Politics and Society, 24: 45-55.

Lewicki, R.J., & Bunker, B.B. (1996). Developing and maintaining trust in work relationships. In R.M. Kramer & T.R. Tyler (Eds.), Trust in organizations:

Frontiers of theory and research (pp. 114-139). Thousand Oaks, CA: Sage Publications.

Liebenau J. and Backhouse J. (1990). Understanding Information: an Introduction, Macmillan, London.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. (1995). "An Integrative Model of Organizational Trust", Academy of Management Review, 20 (3), 709-734.

McKnight, D. H. and Chervany, N. L. (2001). Trust and Distrust Definitions: One Bite at a Time. In Proceedings of the Workshop on Deception, Fraud, and Trust in Agent Societies Held During the Autonomous Agents Conference: Trust in Cyber-Societies, integrating the Human and Artificial Perspectives R. Falcone, M. P. Singh, and Y. Tan, Eds. Lecture Notes In Computer Science, vol. 2246. Springer-Verlag, London, 27-54.

McKnight, D.H., Cummings, L.L. E Chervany, N.L. (1998). Initial Trust Formation in New Organizational Relationships, in «Academy of Management Re-view», vol. 23, n. 3

Misiolek, N.I., N. Zakaria, and P. Zhang (2002). Trust in organizational acceptance of information technology: A conceptual model and preliminary evidence. in Proc. Decision Sciences Institute 33rd Annual Meeting 2002.

Pavlou, P., Tan, Y.H. and Gefen, D. (2003), Institutional Trust and Familiarity in Online Interorganizational Relationship

Ratnasingam, P. (2002). The importance of technology trust in web services security. Information Management & Computer Security, 10(5), 255–260.

Ratnasingam, P. and Pavlou, P. (2002), "Technology trust: the next value creator in B2B electronic commerce", International Resources Management Association Conference - Washington, Seattle.

Reeves, B., & Nass, C. (1996). The media equation. How people treat computers, television, and new media like real people and places. New York: Cambridge University Press.

Rousseau, M.T., Stikin, S.B., Burt, S.B., Carmerer, C. (1998), "Not so different after all: across-discipline view of trust", Academy of Management Review, Vol. 23 No.3, pp.393-404.

RSA (2006), RSA Security research shows volume of business passwords overwhelming end users and hindering IT security efforts, http://www.rsa.com/press_release.aspx?id=7299, retrieved 31.11.2008.

Schläger, C., Ganslmayer, M. (2007) Effects of Architectural Decisions in Authentication and Authorisation Infrastructures. Proc. of the 2nd International Conference on Availability, Reliability and Security (ARES '07), Vienna.

Schläger, C.; Sojer, M.; Muschall, B.; Pernul, G. (2006): Attribute-Based Authentication and Au-thorisation Infrastructures for E-Commerce Providers, pp132-141 Springer-Verlag.

Spagnoletti P., Za S. "Gestire i confini di una organizzazione virtuale", WOA 07, atti VIII Workshop Docenti e Ricercatori di Organizzazione Aziendale, Reggio-Emilia, 8-9 febbraio 2007.

Spagnoletti P., Za S., "Identity management in a cross boarder e-services environment: the LD-CAST case", to appear in Proc. 6th Eastern European eGovernment Days, 23 - 25 April 2008 in Prague

Spagnoletti P., Za S., D'Atri A., (2007). "Institutional Trust and security, new boundaries for Virtual Enterprises", Proc. of 2nd International Workshop on Interoperability Solutions to Trust, Security, Policies and QoS for Enhanced Enterprise Systems, IS-TSPQ2007, Funchal, Portugal.

Stamper R., Liu K., Hafkamp M. and Ades Y. (2000) Understanding the Roles of Signs and Norms in Organisations - A semiotic approach to information systems design. Journal of Behaviour & Information Technology, vol. 19 (1), pp 15-27

Tyler, T.R., & Degoey, P. (1996). Trust in organizational authorities. The influence of motive attributions on willingness to accept decisions. In R.M. Kramer & T.R. Tyler (Eds.), Trust in organizations: Frontiers of theory and research (pp. 331-350). Thousand Oaks, CA: Sage Publications.

Williamson, O. E. (1985). The Economic Institutions of Capitalism. Free Press, New York.

Za S., "Benefici attesi tangibili o intangibili? Il caso delle tecnologie per l'autenticazione federata", itAIS 2007, IV Conference of Italian Chapter of AIS, Oct. 3-4, 2007, Isola di San Servolo, Venice, Italy

IL CASO DELLE ORGANIZZAZIONI VIRTUALI

1. Lo scenario di riferimento

La forte attenzione verso la ricerca di configurazioni efficienti per forme organizzative basate su reti di imprese ed istituzioni, supportate da tecnologie e standard che ne favoriscano l'interoperabilità, è dettata dalle crescenti esigenze del mercato in termini di competitività e dalla complessità dei nuovi servizi e prodotti. In tale ambito, la flessibilità è considerata un attributo necessario per competere con successo sul mercato e l'impresa virtuale è presente in letteratura quale auspicabile forma organizzativa capace di innovare la modalità di cooperazione interorganizzativa.

Un'impresa virtuale è una rete temporanea di piccole e medie imprese che, a seguito di un'opportunità di business sorta sul mercato, si collegano ed operano in modo integrato finché l'opportunità permane. Al raggiungimento degli obiettivi (o al momento in cui questi si dovessero rivelare irraggiungibili) il network si disintegra e le singole imprese tornano ad osservare il mercato per isolare opportunità particolari (Davulcu et al. 1999).

L'impresa virtuale può esser considerata come un sistema debolmente connesso i cui partecipanti definiscono autonomamente le azioni da compiere aggiustandole l'una rispetto all'altra giungendo ad un'azione comune (Grandori 1999). Inoltre quando il business si esaurisce le unità si scollegano e si aggregano secondo nuove modalità dando origine a nuove forme organizzative (Merli e Saccani 1994).

Tra i principali ostacoli allo sviluppo di imprese virtuali sono stati individuati problemi legati ai limiti degli ambienti di supporto alla collaborazione ed

all'inefficienza di alcune configurazioni organizzative. In particolare, "non sono ancora state trovate modalità per favorire la nascita di un clima di fiducia e sicurezza all'interno della comunità" (Barbini 2004).

Più in generale un elemento critico nei processi di implementazione dei sistemi interorganizzativi è individuare la quantità e la qualità delle informazioni che le organizzazioni sono disposte a condividere. Diversi autori hanno dimostrato l'importanza della presenza di una condizione di fiducia reciproca che consenta una forte integrazione anche senza dover costituire una relazione di controllo proprietario tra le controparti (Martinez 2003). Venendo però a mancare, in organizzazioni di tipo virtuale delocalizzate e temporanee, la possibilità di creare relazioni di fiducia basate su contatti interpersonali diretti tra le persone che occupano un ruolo di confine, è necessario individuare meccanismi di altro tipo seppur finalizzati agli stessi obiettivi di creazione delle condizioni di fiducia reciproca. Il nuovo concetto di fiducia che ne deriva, cosiddetto di "fiducia istituzionale", faciliterebbe l'avvio di relazioni mediante sistemi ICT basandosi su tre elementi essenziali (McKnight et al. 1998; Pavlou et al. 2003):

- la percezione di interagire con un sistema tecnico sicuro;
- la presenza di meccanismi interorganizzativi formali;
- la garanzia che le comunicazioni tra i sistemi ICT avvengano in maniera corretta grazie a standard tecnici e procedurali.

In questo scenario, l'intervento di una terza parte potrebbe agevolare la costruzione della fiducia di tipo istituzionale, fornendo un supporto per superare differenze culturali ed eventuali barriere normative che intervengono ad esempio nella collaborazione tra imprese di diversa nazionalità. Il ruolo di tali soggetti terzi dovrebbe infatti garantire, ad esempio creando un marketplace o un portale, che le

transazioni avvengano in un ambiente certificato e "sicuro" in termini di soluzioni tecnologiche adottate per la comunicazione, di regolarità formale degli accordi e di fiducia istituzionale. Ciononostante, la configurazione organizzativa incentrata sulla figura dell'integratore (broker), che rappresenta la più diffusa forma presente in letteratura (Bremer 1999), ha mostrato i suoi limiti sia in termini di capacità di identificare e gestire il business, sia in termini di capacità di gestire e controllare l'intera rete virtuale (D'Atri 2003).

Seppure siano state proposte configurazioni organizzative alternative, quali ad esempio l'ECB (Enabler, Catalyst, Broker) che tendono a ridistribuire i ruoli dei partecipanti ad una impresa virtuale, resta comunque critico il ruolo di quella entità ritenuta stabile per definizione (Enabler), che dovrebbe gestire la comunità online e proporre metodi e strumenti di cooperazione standard, pronti ad essere personalizzati rapidamente nel momento in cui le imprese volessero costituire un'organizzazione virtuale (Barbini e D'Atri 2005).

Un secondo ma non secondario elemento di ostacolo allo sviluppo di organizzazioni virtuali, riguarda invece il rapporto tra organizzazione e clienti ed esula dunque da concetti sino ad ora discussi, quali quello di fiducia istituzionale. In questo caso infatti l'attenzione è rivolta al fatto che caratteristiche di delocalizzazione e temporaneità, proprie dell'organizzazione virtuale, non contribuiscono a favorire la crescita di un rapporto di fiducia tra il cliente ed il fornitore del prodotto o servizio. Si tratta dunque di una criticità riferita al rapporto con i clienti ed al grado di fiducia che questi ripongono verso un'organizzazione temporanea e geograficamente distribuita.

Per far fronte a questo tipo di problemi, nonostante sia stata prevista nella già citata configurazione ECB, la figura del Catalyst che rappresenterebbe l'unica interfaccia

dell'organizzazione virtuale con il cliente, per apparire al mercato come il solo produttore/fornitore del prodotto/servizio realizzato dall'organizzazione virtuale, non riteniamo applicabile questa soluzione a qualsiasi contesto. Infatti, risulta difficile immaginare che, soprattutto in ambiti fortemente delocalizzati ed internazionali, un'unica entità possa gestire efficacemente le interazioni con tutti i clienti, nel rispetto inoltre dei diversi quadri normativi vigenti. Dal punto di vista del cliente invece, potrebbe risultare difficile superare la barriera della fiducia verso una entità remota e temporanea, affidandole i propri dati per ottenere ad esempio un servizio mediante transazioni online (Turner 2003). Alcuni studi considerano infatti tra i principali fattori che ostacolano la diffusione di servizi online, elementi quali la fiducia, la percezione del rischio da parte dei clienti ed i problemi di privacy. Inoltre questo tipo di fattori assume un peso diverso in contesti culturali differenti ed influenza la disponibilità degli utenti ad affidare i propri dati online a soggetti terzi (Dinev et al. 2006).

Quanto descritto rientra in un più ampio quadro di problematiche legate alla tutela della privacy ed al proliferare di sistemi di gestione delle identità. In questo contesto si muovono diversi progetti di ricerca (FIDIS[4] , PRIME[5] , etc.), finalizzati ad individuare i problemi legati all'adozione di sistemi di gestione delle identità e le possibili soluzioni basate spesso sulle stesse tecnologie considerate abilitanti nella letteratura sulle organizzazioni virtuali. Pertanto, tecnologie quali database federati per mezzo dell'XML, standard e protocolli di Internet e sistemi di gestione automatizzata dei workflow, oltre a consentire alle organizzazioni di condividere dati, di porre in essere transazioni, di sviluppare relazioni online e di integrare interi processi inter-organizzativi, potrebbero giocare un ruolo centrale per affrontare le

[4] FIDIS NoE www.fidis.net
[5] PRIME https://www.prime-project.eu/

due classi di problemi sopra descritte (la fiducia istituzionale e la privacy degli utenti).

In particolare, le infrastrutture per l'autenticazione e l'autorizzazione (AAI), sulle quali si basano i servizi di identità federata, introdotti di recente come alternativa alle più diffuse soluzioni centralizzate, potrebbero dar luogo a nuovi approcci nella gestione dei confini delle organizzazioni virtuali. Tra le finalità di questi servizi infatti vi è la creazione di una piattaforma tecnologica sicura ed affidabile che faciliti la collaborazione online di organizzazioni indipendenti e che sviluppi opportunità di nuovi business fondati su partnership "di fiducia", nel pieno rispetto delle norme sulla privacy, locali ed internazionali (Schlaeger e Pernul 2005).

Nel presente lavoro si analizzano nel dettaglio i requisiti di sicurezza delle organizzazioni virtuali, con particolare riferimento all'area di "controllo accessi" prevista dallo standard ISO 17799 (ISO/IEC 2005). Il risultato di tale analisi porta a definire una serie di requisiti di sistema "non funzionali" che saranno messi in relazione con le esigenze di fiducia istituzionale e di privacy dei clienti sopra introdotte.

A questo punto verrà illustrato il progetto di una possibile configurazione organizzativa e del relativo sistema informativo di supporto che, basandosi sulle tecnologie sopra elencate, soddisfi i requisiti descritti. Lo scenario risultante sarà analizzato da un punto di vista concettuale mentre per una verifica empirica si rimanda agli esiti di un progetto europeo nell'ambito del quale si è valutata ed attuata l'implementazione di questo tipo di configurazione.

Da un punto di vista metodologico, il lavoro presenta le caratteristiche di un progetto di "design research". Questa metodologia di ricerca, applicata ai sistemi informativi, prevede un'analisi dell'utilizzo e delle performance dei sistemi progettati, finalizzata

alla comprensione, alla spiegazione ed al miglioramento dei comportamenti all'interno dell'intero sistema informativo (Vaishnavi e Kuechler, 2004). Nonostante questa metodologia sia notoriamente più diffusa in ambito ingegneristico e informatico, negli ultimi anni si assiste ad un ritorno al suo utilizzo da parte dei ricercatori di sistemi informativi (Orlikowski e Iacono, 2001).

2. Quali confini per una organizzazione virtuale?

Le domande di ricerca, finalizzate ad individuare configurazioni innovative per le organizzazioni virtuali, basate su una diversa modalità di gestione dei confini delle stesse, possono essere espresse come segue:

1. quali requisiti "non funzionali", aventi per obiettivo l'incremento della fiducia istituzionale e della privacy nella gestione delle identità, potrebbero guidare nelle scelte architetturali di un sistema informativo di supporto per una organizzazione virtuale?
2. in riferimento a tali requisiti, qual è il possibile ruolo giocato dalle infrastrutture per l'autenticazione e l'autorizzazione (AAI) basate su meccanismi federati di gestione delle identità?

Per fornire una risposta alle precedenti domande, si procederà secondo le fasi della *disegn research* che prevedono, in seguito ad un'analisi concettuale del problema, di intervenire sullo scenario oggetto di studio attraverso l'introduzione di un nuovo artefatto e di studiare lo scenario risultante. Tale processo può essere visto come un ciclo in cui la conoscenza è usata per creare attività e le attività vengono valutate per creare conoscenza (Owen 1997).

I risultati delle varie fasi possono essere raggruppati nelle seguenti categorie (March and Smith, 1995; Rossi and Sein, 2003):

- un insieme di concetti di dominio proposti durante la fase di studio del problema e ridefiniti nel corso della progettazione (*constructs*),
- un insieme di proposizioni e dichiarazioni espresse in relazioni tra costrutti, utilizzate per descrivere il problema e/o la soluzione (*models*),
- un insieme di piani operativi aventi per obiettivo la manipolazione dei costrutti definiti in modo da realizzare le dichiarazioni definite nel modello (*methods*),
- la creazione dell'artefatto visto come una combinazione dei concetti, dei modelli e dei metodi definiti (*instantiation*),
- una teorica sperimentazione dell'artefatto, seguita dall'analisi del suo possibile utilizzo (*better theories*).

3. Requisiti non funzionali per una organizzazione virtuale

Per affrontare il tema della definizione dei requisiti non funzionali, finalizzati ad aumentare la fiducia istituzionale e la privacy nella gestione delle identità, si farà riferimento ad una serie di obiettivi introdotti dallo standard ISO 17799 relativo alle prassi accettate per la gestione della sicurezza delle informazioni. Tale standard elenca diversi controlli suddivisi in dieci aree ed aventi per obiettivo la tutela della riservatezza, integrità e disponibilità delle informazioni, la cui implementazione è strettamente legata al contesto organizzativo in cui si opera. Nel nostro caso, si farà riferimento all'area denominata "Controllo accessi", all'interno della quale sono

descritti 7 obiettivi e 25 controlli. Tra questi, i seguenti obiettivi risultano applicabili al caso delle organizzazioni virtuali:

- *requisiti di business per il controllo accessi*: l'accesso degli utenti alle informazioni ed ai processi di business, dovrebbe essere controllato sulla base dei requisiti di sicurezza e di business stabiliti dai fornitori del servizio. Un insieme di politiche per stabilire tali requisiti, dovrebbe essere definito e condiviso all'interno dell'organizzazione virtuale;
- *gestione accessi*: un insieme di procedure formali dovrebbe prevedere i diversi livelli di autorizzazione per l'accesso alle informazioni. E' possibile infatti pensare che ciascuno dei partner dell'organizzazione abbia regole diverse per la condivisione delle informazioni e per l'erogazione dei servizi. Tali procedure, dovrebbero coprire tutte le fasi dell'intero ciclo di vita dell'utente, dalla registrazione iniziale di un nuovo utente, alla sua identificazione, all'autenticazione ed alla cancellazione degli utenti che non necessitano più di un accesso al sistema informativo;
- *controllo degli accessi alla rete*: un insieme di meccanismi tecnologici dovrebbe garantire la possibilità di controllo su tutti gli accessi ai servizi forniti dall'organizzazione virtuale verso l'interno e verso l'esterno. Itali meccanismi dovrebbero prevedere: una serie di interfacce appropriate tra la rete dell'organizzazione e le reti di altre organizzazioni e le reti pubbliche, meccanismi di autenticazione appropriati per gli utenti ed i dispositivi, il controllo degli accessi ai servizi erogati.

Tali requisiti dunque, nel caso di una organizzazione virtuale, portano a dover effettuare una importante scelta architetturale tra un approccio centralizzato ed uno distribuito. Mentre sono già state ampiamente introdotte le ricadute negative del

primo caso, in termini di fiducia istituzionale, di percezione della privacy da parte degli utenti e di complessità nel rispetto dei vincoli normativi, un approccio decentralizzato per la gestione delle identità lascerebbe al singolo Identity Provider (IdP) le scelte sui meccanismi da adottare per la gestione ed il controllo degli accessi. Tale scelta sarebbe però vincolata alla presenza di una politica condivisa, tra i membri dell'organizzazione virtuale, che stabilisca i requisiti di business e di sicurezza per il controllo degli accessi. In altre parole, si avrebbe un insieme di regole centralizzate ed una serie di procedure e soluzioni tecnologiche distribuite.

Nel seguito della trattazione, si vedrà come l'adozione di sistemi federati per la gestione delle identità, possano rispondere a questo tipo di requisiti.

4. Possibile ruolo delle AAI nelle organizzazioni virtuali

Nelle organizzazioni, l'accesso alle informazioni è comunemente protetto mediante l'uso di regole per il controllo degli accessi (autorizzazione) e di sistemi di autenticazione degli utenti. Infatti, prima di procedere ad una verifica delle autorizzazioni (es. permesso di lettura su un documento, di utilizzo di un'applicazione, etc.), il sistema deve prima verificare l'identità dell'utente. Tecnicamente parleremo di "soggetti" riferendoci a qualsiasi entità (utente o dispositivo) che necessita di un'autenticazione per poter poi avere accesso ad una risorsa. Tali soggetti dunque, interagiscono con sistemi di autenticazione di vario tipo, in maniera dipendente dalla risorsa in questione. In tale ambito, una sorgente di autenticazione è l'autorità che controlla dati e protocolli di autenticazione.

L'autenticazione può avvenire tra soggetti appartenenti alla stessa organizzazione oppure ad organizzazioni differenti. Anche all'interno di una stessa organizzazione è possibile avere diverse sorgenti di autenticazione. Ad esempio, nel caso di Kerberos

(Kohl e Neuman 1993), la sorgente è costituita da un Key Distribution Center (KDC) ed il tipo di autenticazione è basato su nome utente e password. In una Public Key Infrastructure (PKI) invece, la sorgente è la Certification Authority (CA) ed il tipo è detto challenge/response (Ford e Baum 1998). Nonostante sia Kerberos che PKI consentano la presenza di sorgenti multiple di autenticazione, tali sorgenti dovrebbero essere in stretta relazione tra loro. Spesso infatti è necessario che si stabiliscano delle complesse relazioni di fiducia tra le varie sorgenti di autenticazione rendendo tali soluzioni praticamente irrealizzabili ed economicamente non convenienti (Backhouse 2001). Inoltre, guardando alla realtà delle comunicazioni inter ed intra-organizzative, emerge la presenza di diversi tipi di autenticazione quali ad esempio, password, token, certificati digitali e smart card. In questo scenario, una architettura di sicurezza dovrebbe dunque prevedere una singola infrastruttura che gestisca tutti i tipi di autenticazione e che sia predisposta ad accettare dati da un qualsiasi numero di sorgenti.

Nel modello proposto, le diverse sorgenti di autenticazione formano una federazione in cui ciascun membro garantisce l'autenticità di un sottoinsieme di soggetti. Un sistema federato di gestione delle identità, è pensato per rispondere al nuovo modo di concepire le modalità di gestire le autenticazioni online di clienti, aziende ed enti pubblici. In questo caso, con il termine "federato", si fa riferimento ai diversi tipi di autenticazioni e di sorgenti. L'obiettivo dell'organizzazione coinvolta è quello di stabilire, ad un livello di politica e non tecnico, le regole che consentiranno l'interoperabilità dei singoli sistemi di autenticazione. Una volta fissate le regole per assegnare i livelli di fiducia ai sistemi di gestione delle credenziali, per il rilascio delle credenziali stesse e per eseguire il processo di verifica della credibilità, i diversi sistemi coinvolti saranno in grado di condividere dati di autenticazione e di ritenere validi quelli provenienti da altri sistemi. Ad esempio, se un utente volesse accedere al

sito web della sua banca, una organizzazione esterna, potrebbe garantire l'identità dell'utente, verificandola attraverso l'uso di un certificato digitale.

5. Il modello ECB vs il sistema federato

Di seguito si riprende la configurazione organizzativa ECB, descrivendo le funzionalità dei i tre soggetti (Enabler, Catalyst, Broker) per poi proporre come una configurazione organizzativa basata sul concetto di circolo di fiducia risponda agli obiettivi precedentemente esposti.

Di seguito la descrizione dei tre soggetti ECB.

> **Enabler**: è l'attore che sviluppa, gestisce e promuove un ambiente on-line finalizzato all'incontro e cooperazione tra imprese, promuovendo metodi e strumenti flessibili alla personalizzazione nel momento in cui si verifica la necessità di costituire un'organizzazione virtuale all'interno del sottoambiente competitivo di riferimento.
>
> **Catalyst**: è il soggetto che individua l'opportunità di business ed avvia l'organizzazione virtuale, ciò implica che qualsiasi soggetto appartenente al sottoambiente competitivo di riferimento possa divenire catalyst dell'organizzazione virtuale. Esso è anche l'unica interfaccia con l'esterno con cui interagiscono gli utenti.
>
> **Broker** (può coincidere con il Catalyst): ha la responsabilità di coordinare, sincronizzare e controllare il processo virtuale, garantendo alle imprese cooperanti l'accesso ad una vasta base di risorse sempre tutelando le conoscenze critiche private dei partecipanti.

Nella figura 10 è illustrato il rapporto tra i tre soggetti descritti, dove si evince che l'unico punto di accesso ai servizi offerti dall'organizzazione virtuale sia il Catalyst, ponendo l'interrogativo sul rapporto di fiducia che gli utenti richiedenti vi ripongono.

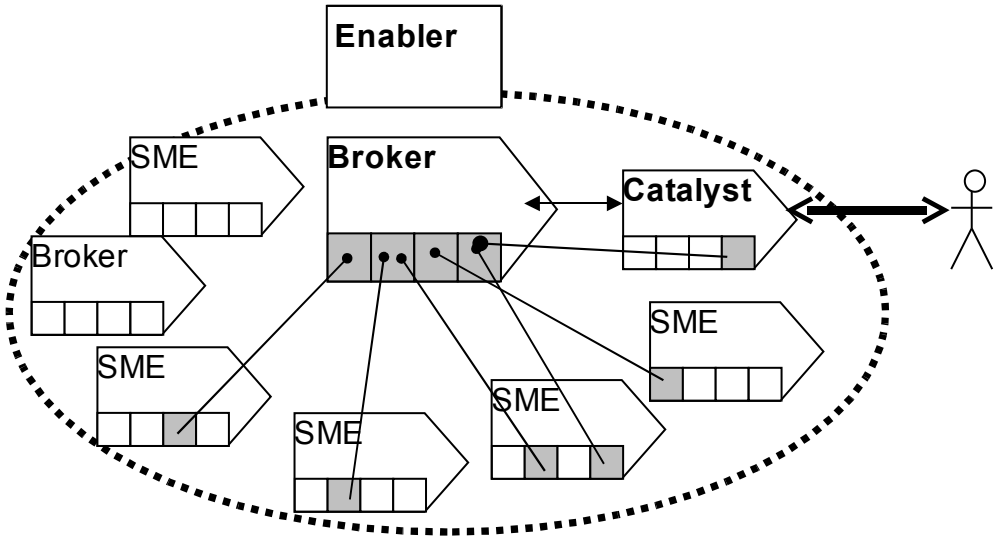

Figura 10. *Enabler, Catalyst and Broker (ECB) (D'Atri, 2003)*

Considerando i confini dell'organizzazione virtuale coincidenti con quelli del Circolo di Fiducia definito nel primo capitolo, questo tipo di architettura sembra rispondere ad entrambi gli obiettivi:

- quali requisiti "non funzionali", aventi per obiettivo l'incremento della fiducia istituzionale e della privacy nella gestione delle identità, potrebbero guidare nelle scelte architetturali di un sistema informativo di supporto per una organizzazione virtuale?
- in riferimento a tali requisiti, qual è il possibile ruolo giocato dalle infrastrutture per l'autenticazione e l'autorizzazione basate su meccanismi federati di gestione delle identità?

Infatti, in una tale configurazione, ciascuno dei Service Provider rappresenterebbe un possibile punto d'accesso per l'utente (vedi figura 11) e la fiducia istituzionale tra i membri dell'organizzazione sarebbe favorita dagli accordi formali previsti dal Circolo di Fiducia. Inoltre i dati personali di registrazione sarebbero conservati dal solo Identity Provider scelto dall'utente, con le ovvie implicazioni per gli aspetti di privacy sopra introdotti.

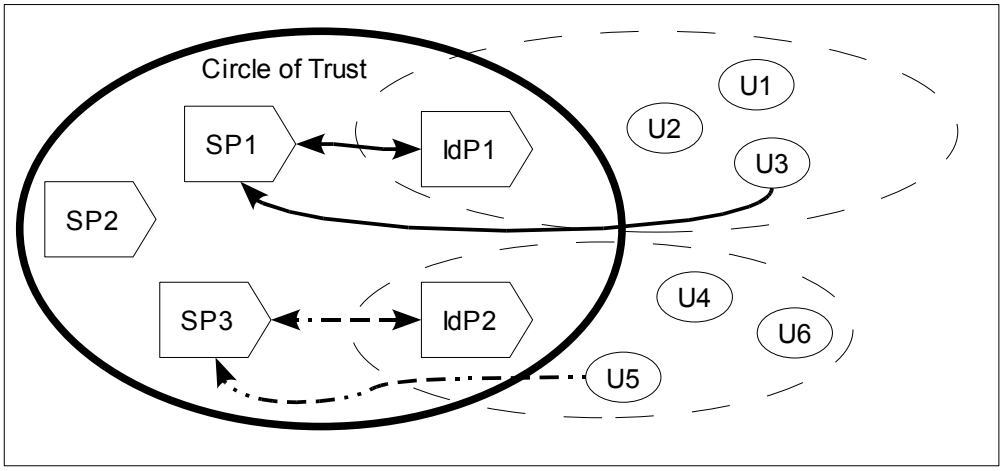

Figura 11. V*irtual organization vs Circle of Trust*

6. Conclusioni

Il lavoro di questo capitolo si basa principalmente sui risultati preliminari del progetto di ricerca europeo LD-CAST finalizzato a favorire la cooperazione tra Camere di Commercio di diversi paesi membri della Comunità Europea. Il progetto LD-CAST infatti prevede la realizzazione di una rete di portali che consentono agli utenti (aziende private e singoli imprenditori) l'accesso a servizi forniti da diverse organizzazioni pubbliche e private.

In tale ambito sono stati prima definiti requisiti non funzionali corrispondenti a quelli esposti nell'articolo e successivamente è stata valutata concettualmente l'opportunità di adottare una architettura federata per la gestione delle identità, del tipo di quella precedentemente descritta (inizialmente si pensava ad un sistema centralizzato).

Nel successivo capitolo si presenterà più in dettaglio il caso LD-CAST e come l'adozione di un sistema federato sia la soluzione ad un insieme di requisiti non-funzionali scaturiti dalla relativa analisi.

7. Bibliografia

Backhouse J. (2001) Assessing Certification Authorities: Guarding the Guardians of Secure E-Commerce? Journal of Financial Crime, 9 (3), pp. 217-226

BARBINI F.M. (2004), Il contributo dell'Impresa Virtuale all'Innovazione Organizzativa, in D'Atri A. (a cura di), Innovazione Tecnologica e Tecnologie Innovative, EtasLibri, Milano.

BARBINI F. M. and D'ATRI A. (2005) How innovative are virtual enterprises? In Proceedings of ECIS 05, The 13th European Conference on Information Systems.

BREMER (1999), Global Virtual Business: A Systematic Approach for Exploiting Business Opportunities in Dynamic Markets, International Journal of Agile Manufacturing, vol.2, issue 1.

CIBORRA, C., MERCURIO, R., DE MARCO, M., MARTINEZ, M. e CARIGNANI, A. [2003] (a cura di), New Paradigms in Organizations, Markets and Society, Proceedings of the XI European Conference on Information Systems, Napoli, 19-21 giugno

D'ATRI, A. (2003). Organising and Managing Virtual Enterprises: the ECB Framework, in Camarinha-Matos, L.M. and Afsarmanesh, H. (eds.). Processes and Foundations for Virtual Organisations. Kluwer Academic Publishers.

DAVULCU, H., KIFER, M, POKORNY, L. R., RAMAKRISHNAN, C. R., RAMAKRISHNAN, I. V., & DAWSON, S. (1999). Modeling and Analysis of Inter-actions in Virtual Enterprises. In Proceedings of the Ninth International Workshop on Research Issues on Data Engineering: Information Technology for Virtual Enterprises (RIDE 1999), IEEE Computer Society, pp.12-18.

DINEV, T., BELLOTTO, M., HART, P., RUSSO, V., SERRA, I., COLAUTTI, C. (2006). Privacy Calculus Model in E-commerce - a Study of Italy and the United States. European Journal of Information Systems, 15, 4, 389-402.

GRANDORI, A. (1999). Interfirm Networks. Routledge, London.

ISO/IEC (2005). ISO/IEC 17799: Information technology- Security techniques - code of practice for information security management

KOHL J. e NEUMAN C. (1993) RFC 1510: The Kerberos Network Authentication Service (V5)

MARCH, S. e SMITH, G. (1995). Design and Natural Science Research on Information Technology. Decision Support Systems 15 (1995): 251 - 266.

MARTINEZ, M., (2004), Organizzazione, informazioni e tecnologie. Il Mulino.

MCKNIGHT, D.H., CUMMINGS, L.L. e CHERVANY, N.L. [1998], Initial Trust Formation in New Organizational Relationships, in «Academy of Management Re-view», vol. 23, n. 3

MERLI G., SACCANI C. (1994), L'Azienda Olonico-Virtuale, Il Sole 24 Ore Libri, Milano

ORLIKOWSKI, W. e IACONO C. (2001). Desperately Seeking the "IT" in IT Research - A Call to Theorizing the IT Artifact. Information Systems Research 12(2): 121-134.

OWEN, C. (1997). Design Research: Building the Knowledge Base. Journal of the Japanese Society for the Science of Design 5(2): 36-45

PAVLOU, P., TAN, Y.H. e GEFEN, D. (2003), Institutional Trust and Familiarity in Online Interorganizational Relationship, Ciborra et al.

ROSSI, M. AND SEIN, M. (2003). Design Research Workshop: A Proactive Research Approach. Presentation delivered at IRIS 26, August 9 – 12, 2003.

SCHLAEGER C. e PERNUL G.. Authentication and Authorisation Infrastructures in b2c e-Commerce. Lecture notes in computer science. Springer-Verlag Berlin Heidel-berg 2005, pag 306-315

TURNER, C.W., How consumers form their judgement of the security of e-commerce web-sites?. Workshop on Human-Computer Interaction and Security Systems, CHI2003, April 5-10, 2003, Fort Lauderdale.

VAISHNAVI V. e KUECHLER W. Design Research in Information Systems, July 2004 http://www.isworld.org/Researchdesign/drisISworld.htm Retrieved October 1st 2006

VENKATRAMAN, N. (1994). IT-Enabled Business Transformation: from Automation to Business Scope Redefinition. Sloan Management Review, Winter, pp.73-78.

VENKATRAMAN N., HENDERSON J. C. (1997), The architecture of virtual organizing: not allow structures but a vibrant strategy, Working Paper, Boston University School of Management.

IL CASO LD-CAST

1. B2G: un ambiente eterogeneo

Il concetta di “Business to Government” (B2G), una variante del modello Business to Business (B2B), riguarda la realizzazione di una piattaforma per lo scambio di informazioni a supporto di attività commerciali tra le imprese e il governo (Galant, 2005). Analogamente al commercio elettronico, l'e-government mira a rendere l'interazione tra il governo e le imprese più facile, conveniente, trasparente e poco costosa (Fang, 2002). Le tecnologie dell'informazione e della comunicazione (TIC) sono usate a tale scopo: per effettuare e automatizzare le interazioni all'interno e tra le imprese e le autorità pubbliche influendo sul modo con cui le imprese fanno affari con il governo.

In genere le prime difficoltà a cui vanno incontro due soggetti intenzionati ad instaurare una relazione sono dovute a problemi di interazione, in questo caso sono particolarmente rilevanti dovuti alla natura estremamente diversa dei soggetti stessi (es.: diversità organizzativa, diverse delle strutture dati, diversi protocolli per lo scambio dei dati).

In generale, l'interoperabilità si riferisce alla capacità di due o più sistemi o componenti di scambiare informazioni e di utilizzare le informazioni scambiate (IEEE, 1990).

La soluzione al problema della eterogeneità si basa sulla selezione e l'attuazione di un adeguato “middleware” che fornisce la funzionalità desiderata (Kajan e Stoimenov, 2005). Il “Middleware” è visto come un importante elemento architetturale di sostegno alle applicazioni distribuite. Il ruolo del “middleware” è

quello di presentare un unico modello di programmazione che risolve il problema della eterogeneità.

In un ambiente B2G, un middleware consiste di vari protocolli standardizzati che descrivono come i messaggi vengono scambiati tra le imprese e i governi, i protocolli coinvolti per il trasporto, alcuni aspetti di sicurezza, e altre funzioni (Bussler , 2001).

Negli ultimi anni in Europa si è assistito a diverse iniziative di partnership e di rapporti B2G, nate per affrontare diverse sfide, a livello locale, nazionale e regionale. In questo contesto si guarda al concetto di partnership come un'alleanza multi-settoriale in cui individui, gruppi o organizzazioni decidono di lavorare insieme per adempiere un obbligo preciso o per effettuare un compito specifico, e condividere rischi e vantaggi.

Il progetto LD-CAST mira a supportare la cooperazione transfrontaliera tra le camere di commercio (CC), al fine di sostenere lo sviluppo delle iniziative delle società private dei paesi partner. Il progetto porterà a costruire una rete europea di portali LD-CAST che consentirà agli utenti finali (in particolar modo alle imprese private) l'accesso (in modalità “seamless”) ai servizi forniti dagli enti pubblici registrati in ciascun portale.

Questa rete sarà basata su un framework comune, al fine di realizzare e sfruttare un unico modello di piattaforma a tutti i livelli (europeo, nazionale, regionale e locale), compatibile con le linee guida EIF[6] (European Interoperability Framework) senza richiedere specifici cambiamenti sia da un punto di vista delle procedure e sia da un punto di vista del sistema delle organizzazioni partecipanti.

[6]http://ec.europa.eu/idabc/servlets/Doc?id=31597

2. LD-CAST: System Overview

L'obiettivo finale del sistema è di fornire servizi e-Business agli imprenditori. Tali servizi possono coprire in linea di principio tutti i tipi di servizi relativi alle attività di business che possono essere eseguite completamente on-line.

Sistemi simili esistono già, ma consistono in portali che forniscono informazioni minimali permettendo un insieme di operazioni predefinite, specialmente a livello nazionale, con un limitato grado di cooperazione tra le PMI al livello transnazionale.

Attraverso l'utilizzo di tecnologie semantiche, questo sistema è in grado di recuperare i servizi offerti da diversi "e-government supplier" ed aggregarli insieme a formare nuovi servizi in maniera (semi)automatica, selezionando quelli appropriati che meglio soddisfano le richieste dell'utente, senza limitarsi ad un set di servizi o combinazioni strettamente pre-programmate e determinate.

Volendo riassumere in poche parole, il sistema LD-CAST si basa sulle seguenti funzionalità: un imprenditore usa il servizio LD-CAST come punto di partenza per effettuare la sua richiesta. I servizi all'utente sono forniti dal sistema attraverso la selezione, la richiesta e la composizione di (WEB)service offerti dai diversi service provider.

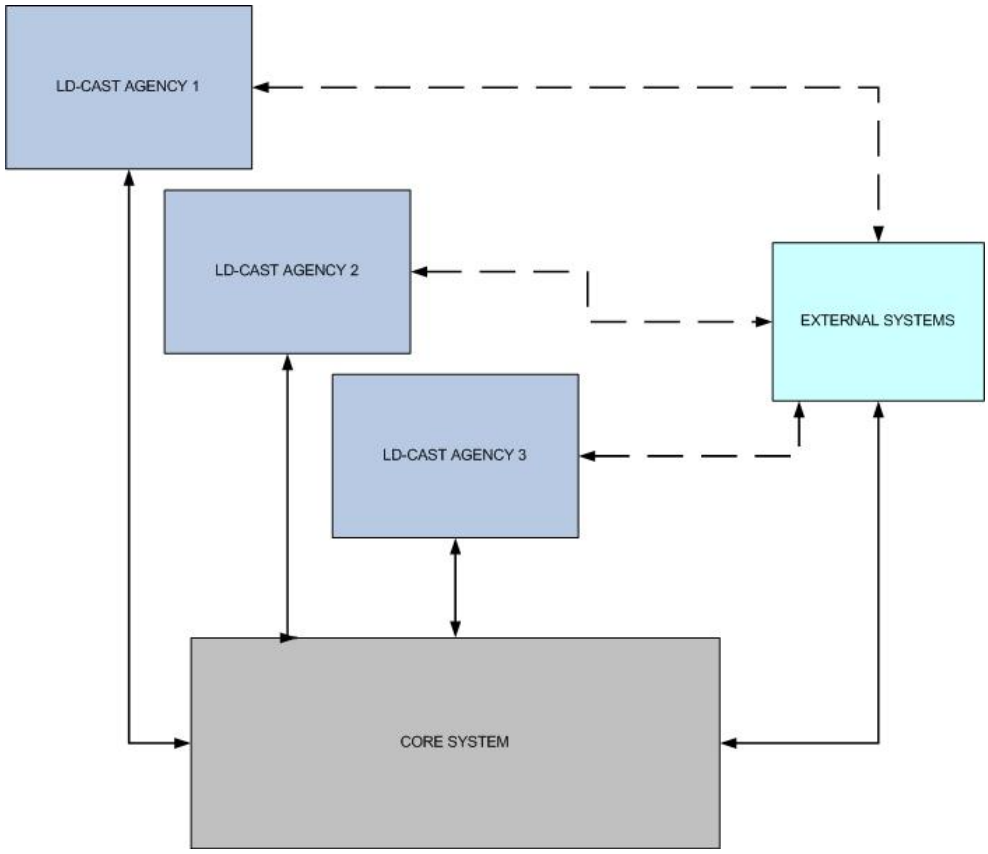

Figure 12 *LD-CAST main entities*

Seguendo un approccio top-down, è possibile identificare tre principali entità nello scenario LD-CAST (figura 12): *LD-CAST Agency*, *Core System* e *External Systems*.

LD-CAST Agencies (definita Agency dora in avanti) agisce come punto di connessione tra l'imprenditore e i servizi offerti dalla piattaforma LD-CAST (core system). Ogni organizzazione che vuole entrare a far parte di LD-CAST svolgendo il ruolo di Agency, dovrà avere le seguenti responsabilità:

- la gestione locale degli utenti che potranno accedere ai servizi del core system, agendo da identity provider all'interno del sistema federato

implementato nel progetto; le linee tratteggiate tra l'External Systems e l'Agency rappresentano l'interazione tra queste due entità riguardante la fase di autorizzazione dell'utente;

- gestire i pagamenti tra l'utente finale e l'Agency per l'accesso ai servizi del Core System;
- fornire informazioni relative a LD-CAST.

L'utente finale (l'imprenditore) esegue la propria registrazione e identificazione seguendo le procedure interne relative all'Agency coinvolta. Per esempio, un Agency può richiedere di fornire informazioni relative alla carta di identità, un altra può invece permette di utilizzare certificati digitali.

L'Agency abilita l'utente finale ad accedere ai servizi del Core System che interagirà con la stessa Agency per controllare l'identità dell'utente stesso.

Inoltre l'utente paga direttamente l'Agency per l'accesso al servizio, mentre il Core System traccia il processo di accounting con l'External System.

LD-CAST Core System può essere visto come una piattaforma complessa che offre diversi servizi a diverse categorie di utenze con l'obiettivo di supportare l'utente finale nelle attività di business.

External Systems fornisce il servizio che sarà gestito ed eventualmente combinato dal core system per soddisfare la richiesta dell'utente.

3. Il sotto-sistema per la gestione delle Autenticazione e Autorizzazione

Da un punto di vista della sicurezza, una delle principali questioni scaturite dall'analisi dei requisiti è relativa alla scelta dell'infrastruttura da adottare per la gestione delle utenze: centralizzata o decentralizzata (federata).

L'obiettivo è di abilitare l'utente (principalmente imprenditori privati) all'accesso in "seamless mode" ai servizi forniti dalle pubbliche organizzazioni registrate in ogni LD-CAST portal.

L'insieme dei requisiti non funzionali definiti durante la prima fase del progetto, possono essere classificati come segue:

1. identity management: relativamente alla gestione centralizzata delle informazioni legate alle identità degli utenti sono emerse potenziali questioni legali che hanno portato all'adozione di un approccio decentralizzato o federato per la gestione delle identità;
2. identification: meccanismi differenti sono accettati per completare la fase di registrazione da ogni Local Agency (i.e. certificati digitali, smart card, certified e-mail message o "face-to-face"). Ogni Local Agency si rende responsabile del processo di identificazione del proprio utente registrato;
3. authentication: un meccanismo Single-Sign-On fornisce all'utente l'accesso a tutto il sistema LD-CAST (in accordo con le credenziali relative). L'autenticazione (authentication) può essere basata anche semplicemente su una coppia di username e password;
4. meccanismi di autorizzazione (authorisation mechanism): dipendono dalle regole e dalle policy di ogni service provider (SP).

In questo scenario, la selezione e l'implementazione di una infrastruttura federata per la gestione delle autenticazioni e autorizzazioni (AAI) ha risolto il problema dell'autenticazione e autorizzazione inter-organizzativa.

Infatti, l'obiettivo di un sistema federato è di costituire una piattaforma sicura ed affidabile a supporto della cooperazione on-line tra organizzazioni indipendenti al fine di sfruttare opportunità di business (Schlaeger and Pernul 2005).

4. Descrizione dell'Architettura

Il concetto di “circolo di fiducia” (“circle of trust” o federazione), descritto nel primo capitolo, è definito come un gruppo di organizzazioni che hanno stabilito degli accordi sulle modalità di interazione nella gestione delle identità degli utenti. Una volta che un utente effettua l’autenticazione presso un Identity Provider (IdP) appartenente al Circolo di Fiducia, lo stesso utente può usufruire dei servizi forniti da qualsiasi Service Provider (SP) appartenente allo stesso Circolo.

Standard e linee guida prese comi riferimento si trovano nella documentazione del progetto Liberty Alliance.

Liberty Alliance Project, è stata costituita per promuovere lo sviluppo di tali standard e specifiche, implementando un sistema federato per la gestione delle identità basato su prodotti e tecnologie che supportano i protocolli definiti. Liberty Identity Federation Framework (ID-FF) comprende la fase 1 delle specifiche Liberty (“Liberty Specifications”) e fornisce il meccanismo di single sign-on e il collegamento di separati account con un gruppo di service provider all'interno del circolo di fiducia.

Riprendendo la definizione dei soggetti descritti nel primo capitolo, si identificano le seguenti tre tipologie:

1. Identity provider (IdP) – nel quale risiedono i dati di registrazione degli utenti (in questo caso le camere di commercio)
2. Service Provider (SP) – fornitore di uno o più servizi (qualunque LD-CAST SP registrato che fornisce uno o più servizi)
3. User agent (UA) – l'applicazione dell'utente che comunica con l'IdP o con il SP (per esempio il web browser)

L'interazione tra i soggetti, come descritto nella figura 13, può avvenire mediante:

- Web services (comunicazione diretta tra IdP e SP),
- Web redirection (l'IdP ed il SP comunicano indirettamente attraverso lo user agent),
- Schemi e Metadati (utilizzati nella comunicazione tra SP ed IdP).

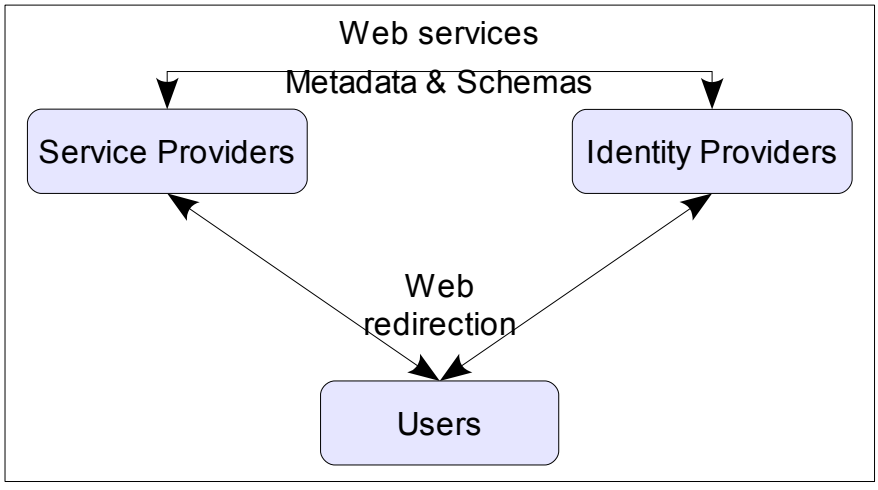

Figure 13 *Subject's interaction*

Per esempio, quando un utente vuole richiedere un servizio LD-CAST, la camera di commercio presso cui lui è registrato (tramite per esempio firma digitale), garantirà che l'utente richiedente è colui che dice di essere.

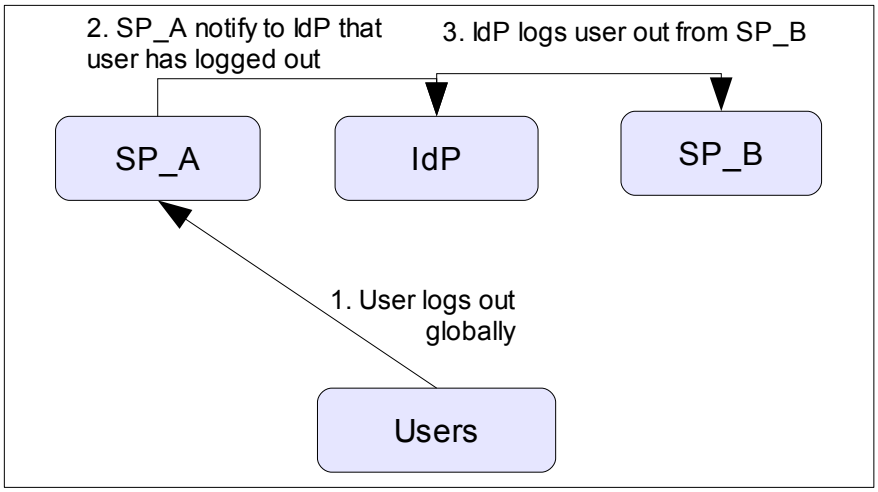

Figure 14 *logout activity*

Allo stesso modo, quando l'utente effettua il logout da un SP, il SP stesso comunica all'IdP responsabile dell'handle dell'utente l'avvenuto logout. L'IdP successivamente propaga l'operazione di logout a tutti i SP che sono stati coinvolti durante la sessione dalle attività dell'utente (vedi figura 14), tenendo traccia dell'handle utilizzato in modo da non generarne casualmente uno uguale.

Nella figura seguente viene illustrato un sequence diagram che rappresenta la fase di autenticazione e il processo di creazione dell'handle, partendo dal login dell'utente presso un SP appartenente al circolo di fiducia.

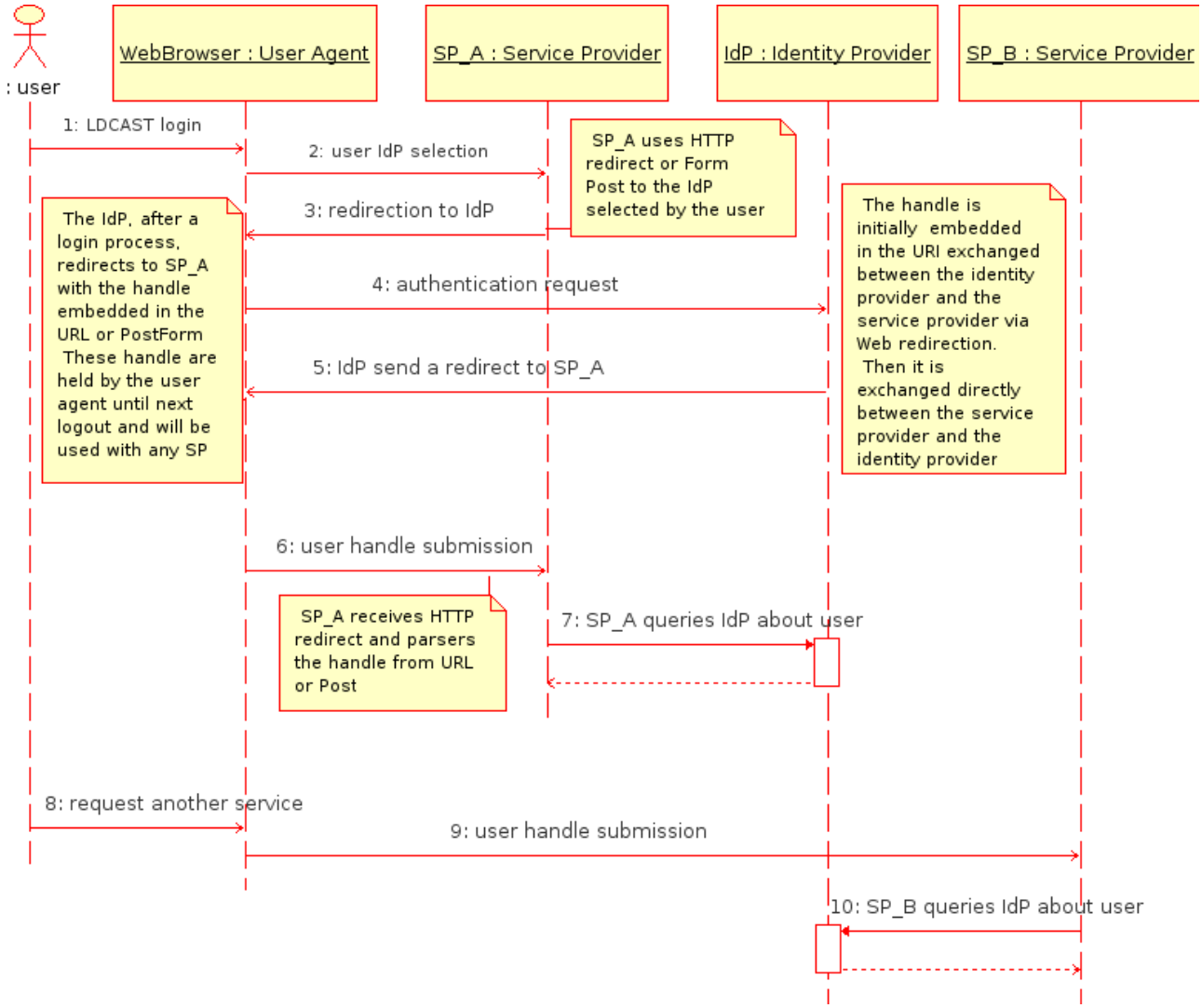

Figure 15 *Communication architecture*

Nella schema in figura 15, SP_A rappresenta LD-CAST Core System in cui l'utente fa riferimento attraverso lo user agent (il browser). Quando esegue il login all'interno del circolo di fiducia, il proprio IdP (la camera di commercio a cui appartiene) crea un “handle” e lo invia allo User Agent. Questo Handle è mantenuto dallo User Agent sino al successivo logout ed è accettato da ogni IdP o SP appartenenti al circolo.

Ogni volta che l'utente cercherà di accedere ad un trusted SP, lo User Agent invia lo "user handle" al SP. Successivamente il SP comunica con L'IdP dell'utente per ottenere le credenziali ed eventuali altri attributi previsti per l'erogazione del servizio richiesto (senza alcuna altra operazione di login). Infine, quando l'utente esegue il logout dall'SP, l'IdP di competenza viene informato e l'operazione di logout è propagata a tutti i SP che sono stati coinvolti durante la sessione dalle attività dell'utente. Lo user handle viene memorizzato in modo da non generare duplicati.

Questa architettura permette all'utente di eseguire il login una sola volta durante una sessione (SSO) e gli permette di interagire con ogni altro SP o IdP all'interno del circolo di fiducia senza ulteriori operazioni di login. Inoltre i dati di registrazione risiedono e sono gestiti dall'IdP scelto da ogni utente, con notevoli vantaggi relativi alla privacy.

Il concetto di circolo di fiducia si incastra con i requisiti non funzionali descritti precedentemente. Le funzionalità base di questa soluzione sono strettamente legate alle interazioni tra utente e proprio IdP (i.e. camera di commercio) durante il processo di autenticazione e autorizzazione. Questi tre interazioni sono: autenticazione dell'utente, richiesta di accesso e invio degli attributi e autorizzazione dall'IdP al SP.

Di seguito sono descritte dettagliatamente queste interazioni.

- 1. **LD-CAST login**. Nello step 1, l'utente tramite un HTTP User Agent, esegue una richiesta HTTP per accedere ad una risorsa protetta senza aver ancora eseguito il login.
- 2. **Identity Provider Selection**. Nello step 2, viene chiesto all'utente di selezionare il proprio Identity Provider nella lista degli IdP appartenenti al circolo di fiducia.

- 3-4. **Redirections to Identity Provider and Authentication Request**. Nello step 3 e 4, il service provider (LD-CAST portal) restituisce un redirect allo user agent con una “Authentication Request” all'identity provider selezionato dall'utente (è possibile anche implementare un servizio che possa in modalità interattiva individuare l'IdP di appartenenza)
- 5-6. **Identity Provider sends redirect to the Service Provider and the user submits the handle**. Nello step 5, l'utente è identificato dall'IdP con una serie di procedure. L'identity provider rilascia un messaggio <samlp:Response> o uno o più SAML artifact per essere consegnati dallo User Agent al Service Provider (step 6). Possono essere usati sia il prodilo SAML 1.1 Browser/POST sia il profilo Browser/Artifact. Se è usato il Browser/POST profile, allora o una (o più) “assertions” o un “error respons” vengono passati tramite lo UA al SP. Se invece si utilizza Browser/Artifact profile allora una o più SAML “artifacts” sono passati attraverso lo UA al SP e successivamente il SP comunica direttamente con l'IdP per risolvere gli “artifacts” in “assertions”
- 7. **Service Provider queries the Identity Provider about the user**. Nello step 7, il service provider può (eventualmente) usare il subject dell'“authentication assertion” ricevuto allo step 6 per inviare un <samlp:AttributeQuery> (all'interno di un messaggio <samlp:Request>) verso un attribute authority associata con un identity provider. A questo punto l'attribute authority associata con l'identity provider gestisce la query <samlp:AttributeQuery> e restituisce un messaggio <samlp:Response>, possibilmente contenente uno o più assertions contenenti attributi da applicare all'utente. A questo punto, il service provider può rispondere allo

user agent con un proprio errore, o può stabilire un proprio “security context” per il richiedente e restituire la risorsa richiesta.

- 8. **User requests other services**. Nello step 8, una nuova richiesta è eseguita da parte dell'utente all'interno della stessa sessione.
- 9-10. **Handle submission and IdP query**. Negli step 9 e 10, l'interazione descritta negli step 6 e 7 sono ripetute con un differente Service Provider appartenente allo stesso circolo di fiducia.

5. Scelta della soluzione tecnologica

Sono disponibili diverse implementazioni tecnologiche per questo tipo di architettura sia commerciale sia open-source.

Una classificazione aggiornata dei progetti open-source relativi alla gestione delle identità è fornita da Safehaus[7]. La soluzione adottata all'interno del progetto LD-CAST è quella fornita da Shibboleth[8]; di seguito ne verranno descritte le caratteristiche.

Shibboleth

Si tratta di una middleware opensource le cui funzionalità sono basate su standard definiti; fornisce il Web Single SignOn (SSO) tra o all'interno dei confini organizzativi. Permette l'accesso alle risorse presenti sui siti, ricevendo le informazioni legate all'autorizzazione per l'accesso on-line alle risorse, in modo da preservare la privacy.

[7]http://docs.safehaus.org/display/HAUS/Home
[8]http://shibboleth.internet2.edu/

Shibboleth implementa le specifiche OASIS SAML v1.1, fornendo la funzionalità di Single SingOn federato e un framework per lo scambio di attributi. Inoltre fornisce delle funzionalità estese relative alla privacy, premettendo al browser dell'utente e al suo homesite di controllare le informazioni degli attributi prima di essere rilasciati ad ogni Service Provider.

Avendo gli accessi basati su Shibboleth si semplifica la gestione delle identità e dei permessi di accesso lato Identity Provider e Service Provider.

Questa soluzione è sviluppata in un ambiente open, liberamente disponibile e realizzata sotto la licenza Apache Software License.

Di seguito si descrivono le principali componenti dell'architettura di Shibboleth:

- **Identity Provider:** è un entità che si occupa di autenticare gli utenti e di produrre le "assertion" di autenticazione e gli attributi in conformità con (Maler et al. 2003) e i profili SAML Browser/POST o Browser/Artifact in conformità con (Maler et al. 2003a). Consiste di componenti funzionali basate sul modello SAML, un authentication authority ed un attribute authority, assieme a un servizio "inter-site transfer", definito dal Browser profiles, e ad un servizio single sign-on, definito dalle specifiche. Notare che fisicamente il servizio di single sign-on e quello di "inter-site transfer" potrebbero risiedere nella stessa location.
- **Authentication Authority:** è un servizio definito su SAML che si occupa di emettere le assertion relative all'autenticazione da consegnare alle parti interessate (service provider, nel caso di Shibboleth). Shibboleth non specifica come le procedure di autenticazione devono avvenire; l'authority comunica con il servizio che effettua l'autenticazione dell'utente da cui si producono le assertion relative a tale evento. L'unico uso che è possibile fare

delle assertion relative all'autenticazione è in conformità con i profili Browser/POST e Browser/Artifact. Come risultato, l'authentication authority è non richiesta (NOT REQUIRED) per processare i messaggi SAML <samlp:Request> contenenti gli elementi <samlp:AuthenticationQuery> o <saml:AssertionIDReference>, ma si potrebbe decidere di utilizzarla. Inoltre i profili Browser/POST e il Browser/Artifact non richiedono specificatamente all'authentication authority di ricordare le assertion che essa emette in un periodo di tempo esteso, comunque è possibile implementare anche questo.

- **Inter-site transfer service:** è una risorsa HTTP controllata dall'identity provider che interagisce con l'authentication authority per emettere l'HTTP response ed inviarlo al browser dell'utente in conformità con i profili SAML Browser/POST o Browser/Artifact. Nel caso del profilo Browser/POST, l'HTTP response contiene i controlli sul form necessario a trasmettere un "short-lived authentication assertion" all'interno del messaggio <samlp:Response> al servizio di assertion del service provider. Nel caso del profilo Browser/Artifact, l'HTTP response contiene un "Location header" che esegue un redirect del browser al servizio di assertion del service provider. L'URL del redirect contiene una o più "URL-encoded SAML artifacts". Inter-site transfer service ed il SSO service potrebbero risiedere all'interno dello stesso HTTP endpoint.
- The **attribute authority** è un servizio basato su SAML che supporta il binding e la gestione dei messaggi SAML <samlp:Request> contenenti l'elemento <samlp:AttributeQuery>. Questo servizio emette le attribute assertion ai service provider in modalità di muta autenticazione. Le implementazioni sono basate sui protocolli SSL/TLS[9] o SAML message

[9]http://www.ietf.org/rfc/rfc2246.txt

signatures per autenticare reciprocamente lo scambio di informazioni. Shibboleth inoltre richiede che il controllo del rilascio degli attributi al service provider sia disponibile sia agli amministratori del sistema e sia agli utenti. Quindi una Shibboleth attribute authority deve avere la capacità di autenticare le richieste e deve implementare alcune forme di controllo degli accessi governando il rilascio di specifici attributi e valori in accordo con specifiche direttive e specifiche richieste dei service provider. Soggetti a questi vincoli, ogni meccanismo di controllo degli accessi potrebbe essere supportato. Una Shibboleth attribute authority potrebbe implementare il supporto per <saml:SubjectConfirmation> (messaggio di conferma) quando vengono gestite le query, ma questo non è richiesto. In pratica, può restituire un errore quando vengono presentate delle query contenenti metodi di conferma non supportati o quando viene chiesto di produrre assertion che li contengono. In fine una Shibboleth attribute authority deve supportare lo scambio di attributi descritto.

- A **single sign-on (SSO) service** è una risorsa HTTP controllata dall'identity provider che riceve e tratta le richieste di autenticazione inviate attraverso il browser dal service provider. Il servizio SSO inizializza il processo di autenticazione, ed eventualmente ridirige il browser al servizio inter-site transfer. Il servizio SSO è uno specifico servizio di Shibboleth che non è definito dal SAML 1.1. Supporta un "normative protocol" per permettere la funzionalità di SSO ad un service provider, che in SAML 1.1 non è definito. Un identity provider potrebbe esporre alcuni SSO service endpoints. Ogni endpoint dovrebbe essere protetto dai protocolli SSL/TLS[10].

[10]http://www.ietf.org/rfc/rfc2246.txt

- **Service provider:** è un entità che fornisce un servizio web-based, applicazioni, o risorse soggetti ad autorizzazione o a personalizzazioni sulla base del security context stabilito dai profili SAML Browser/POST o Browser/Artifact. Consiste in una o più servizi di assertion, definiti dai browser profile, e potrebbero includere gli attributi del richiedente. Ad ogni service provider deve essere assegnato un unico identificativo (identifier), o provider ID. L'identifier deve essere un URI[11] di non oltre 1024 caratteri. Usando URL "https" per questo scopo potrebbe essere vantaggioso per la pubblicazione di metadata.
- **Artifact resolution service:** è un SAML protocol endpoint controllato dall'identity provider che riceve le richieste dal service provider e risolve un SAML artifact nella corrispondente assertion in conformità con il profilo Browser/Artifact. Il servizio supporta la gestione dei messaggi SAML <samlp:Request> contenenti <samlp:AssertionArtifact> in modalità di mutua autenticazione. Le implementazioni si basano su SSL/TLS o SAML message signatures per permettere lo scambio di messaggi in muta autenticazione.
- Un servizio di assertion è una risorsa HTTP controllata dal service provider che gestisce la sottomissione di form attenenti al profilo SAML Browser/POST o HTTP GET requests attenenti al profilo SAML Browser/Artifact per stabilire un nuovo security context. Assumendo che la costituzione di un nuovo security context vada a buon fine si ridirige lo user agent alla risorsa residente sul service provider.
- Shibboleth integra il profilo SAML browser con un scambio di attributi. Un service provider potrebbe utilizzare un SAML protocol compatibile per inviare SAML <samlp:Request> messages contenenti

[11]http://www.ietf.org/rfc/rfc2396.txt

<samlp:AttributeQuery> alle Attribute Authority e gestire l'attribute assertion risultanti. Le implementazioni tipiche basate su SSL/TLS o su SAML message signatures per autenticare reciprocamente lo scambio

6. Architettura vs Requisiti

La tabella seguente riassume la corrispondenza tra i requisiti di sicurezza del progetto LD-CAST e le funzionalità fornite dalla soluzione descritta precedentemente.

LD-CAST requirement	Federated identity architecture
Local Agency in charge of the identification of his own registered users	Identity Provider are responsible for the identification and authentication of their own users
Single-Sign-On	Simplified sign-on is supported both within a circle of trust and across circles of trust.
Management of different authorization mechanisms	SAML is an XML standard for exchanging authentication and authorization data
decentralization of users data	A federated identity architecture does not require the user's personal information to be stored centrally

Tabella 3. *LD-CAST requirement vs federated identity architecture*

Le questioni di sicurezza e di gestione delle identità pongono nuove sfide nel contesto e-service trans-nazionali. I sistemi Federati per la gestione delle identità (Federated Identity Management Systems) sembrano andare bene con i requisiti scaturiti durante la relativa fase di analisi nel progetto, in termini di strumento istituzionale per la fiducia e la sicurezza. Tuttavia l'adozione di tali soluzioni tecnologiche è un compito non banale soprattutto quando organizzazioni eterogenee

devono e vogliono cooperare. Infatti affiorano nuovi vincoli relativi all'interoperabilità tecnologica, accordi formali e relazioni (informali) di fiducia.

Il concetto di circolo di fiducia (Circle of Trust) e le specifiche fornite dal progetto Liberty Alliance soddisfano i requisiti non funzionali emersi nel progetto LD-CAST.

Pertanto, le funzionalità di base di tale soluzione sono strettamente legate alle tre interazioni tra un utente, il suo Identity Provider (cioè la locale Camera di Commercio) e di un Service Provider generico durante il processo di autenticazione e autorizzazione. Questi tre interazioni fondamentali sono l'autenticazione degli utenti, la richiesta di accesso a risorse e la consegna di attributi di autorizzazione dall'Identity Provider al Service Provider.

7. Bibliografia

Bussler, C. (2001) “B2B Protocol Standards and Their Role in Semantic B2B integration engines”, IEEE Data Engineering Bulletin, 1 (2001), pp. 3-11.

Galant, V. (2005) “Blending E-Commerce Theory and Application,” IEEE Distributed Systems Online, vol. 6, no. 1.

IEEE, Institute of Electrical and Electronics Engineers, (1990) IEEE Standard Dictionary: A Compilation of IEEE Standard Computer Glossaries, IEEE, NY.

Kajan, E. and Stoimenov, L. (2005) “Towards and Ontology-Driven Architectural Framework for B2B”, Communications of the ACM, December 2005, Vol. 48, No 12, pp. 60-66

Bussler, C. (2001) “B2B Protocol Standards and Their Role in Semantic B2B integration engines”, IEEE Data Engineering Bulletin, 1 (2001), pp. 3-11.

SCHLAEGER C. e PERNUL G.. Authentication and Authorisation Infrastructures in b2c e-Commerce. Lecture notes in computer science. Springer-Verlag Berlin Heidelberg 2005, pag 306-315

E. Maler et al., (Maler et al. 2003) Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML). OASIS, September 2003. Document ID oasis-sstc-saml-core-1.1 http://www.oasis-open.org/committees/security/

E. Maler et al., (Maler et al. 2003a) Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS, September 2003. Document ID oasis-sstc-samlbindings-profiles-1.1 http://www.oasis-open.org/committees/security/

IL CASO DELLE TECNOLOGIE PER L'AUTENTICAZIONE FEDERATA: BENEFICI ATTESI TANGIBILI vs INTANGIBILI

1. Introduzione

Nell'ambito delle relazioni inter-organizzative, il concetto di fiducia rappresenta un elemento di particolare rilievo in quanto appartenente a quell'insieme di fattori che determinano la fattibilità stessa delle transazioni intese come scambi di prodotti o servizi tra diversi soggetti. Un crescente interesse nell'area dei sistemi informativi verso questi argomenti trova riscontro nella presenza di diverse definizioni di "fiducia" e di studi volti a comprendere fattori e meccanismi che ne influenzano la crescita nonché di indicatori per una stima del grado di fiducia in determinati contesti. A titolo di esempio possiamo citare la sicurezza dell'ambiente in cui avvengono gli scambi ed i meccanismi reputazionali quali elementi sui quali è possibile intervenire per modificare il livello di fiducia. Tra le definizioni presenti in letteratura vi sono quelle più orientate a considerare la fiducia come elemento che dipende da credenze, atteggiamenti, intenzioni e comportamenti (Bhattacherjee 2002) ed altri che invece si concentrano maggiormente su aspetti legati al singolo individuo come la predisposizione al rischio (Mayer et al. 1995). Relativamente a questo secondo approccio, sebbene la fiducia possa essere sempre riconducibile ad un insieme di "credenze" o "percezioni", essa risulta comunque legata agli attributi riconosciuti al fiduciario, di cui si possono individuare caratteristiche quali l'integrità, la benevolenza e la competenza (Mayer et al. 1995):

- Integrità: la convinzione che il fiduciario aderisca ad un insieme di principi e regole di scambio accettate da colui che ripone la fiducia.

- Benevolenza: è il grado di buona fede riposta nel fiduciario.
- Competenza: indica la percezione delle competenze, capacità e "know how" viste nel fiduciario.

In questo lavoro la fiducia è considerata come costituita da un'insieme di convinzioni, scaturite da esperienze positive di interazione (fiducia personale o sociale) o da rapporti formali (fiducia istituzionale).

Un esempio nel panorama italiano può essere l'insieme di rapporti tra le imprese facenti parte di un distretto industriale: la fiducia tra le parti è supportata dal fatto che le imprese agiscono in un territorio ben definito, comunque nazionale, quindi i rapporti si basano spesso su simile cultura, tradizioni, valori comuni, non trascurando il fatto che esiste un unico insieme di norme che regola tali rapporti. Considerando questo caso, nel momento in cui viene a mancare la prossimità territoriale, in che modo si potrebbe instaurare lo stesso livello di fiducia verso soggetti distanti e spesso sconosciuti? E' il caso ad esempio di filiere di organizzazioni che erogano servizi in contesti delocalizzati e secondo modalità fortemente basate sulle tecnologie ICT. In tale ambito assumono importanza, nel determinare il livello di fiducia percepita dalle parti (percezione del clima di fiducia durante le transazioni (Ciborra 1989)), le modalità con cui si gestiscono e scambiano le informazioni.

In questo contesto, particolare importanza ricoprono i sistemi di autenticazione e autorizzazione all'interno di un network di imprese, dove ogni impresa può ricoprire il ruolo di fornitore e/o richiedente di uno o più servizi. In questo ultimo caso sarà tale impresa a dover gestire le informazioni legate alle identità dei richiedenti (siano essi propri clienti o propri dipendenti) nella richiesta del servizio verso terzi. In questo scenario, coloro che richiedono il servizio riporranno maggiore o minore

fiducia nell'azienda erogatrice in base a diversi aspetti legati alla gestione delle proprie informazioni.

Lo scopo di questo studio è di investigare le ragioni dell'adozione di questo tipo di sistema nei diversi contesti organizzativi, esaminando i benefici scaturiti dall'utilizzo di questa particolare tecnologia, soffermandosi non solo sugli aspetti intangibili (come fiducia, sicurezza, privacy, usabilità), ma anche sugli aspetti tangibili (riduzione dei costi di gestione, aumento delle performance dei processi).

Nel prossimo paragrafo, adottando un metodo di ricerca ibrido, combinando quello quantitativo e quello qualitativo (Gable 1994, Kaplan and Duchon 1988, Lee 1991, Mingers 2001, Ragin 1987) seguendo un approccio interpretativo (Walsham 1993), verranno considerati inizialmente i casi di adozione documentati (raccolti una volta ogni 10 mesi a partire da novembre 2006), al fine di avere il trend di diffusione dell'utilizzo di questo sistema nei vari settori, successivamente ne verranno analizzati 25[12] in dettaglio, selezionati tra i settori in cui vi è una più alta diffusione.

2. Casi di studio

Questo studio parte dall'analisi dell'adozione del sistema Federato per la gestione delle identità basata sul monitoraggio dei casi menzionati sul sito ufficiale del progetto Liberty Alliance. Di seguito vengono forniti tre grafici basati su tre rilevazioni (Novembre 2006, Agosto 2007 e Giugno 2008) che illustrano il numero di casi di adozione per ogni contesto di riferimento ed i nuovi contesti per ogni anno.

[12] I casi selezionati sono stati anche influenzati dalla disponibilità della documentazione relativa

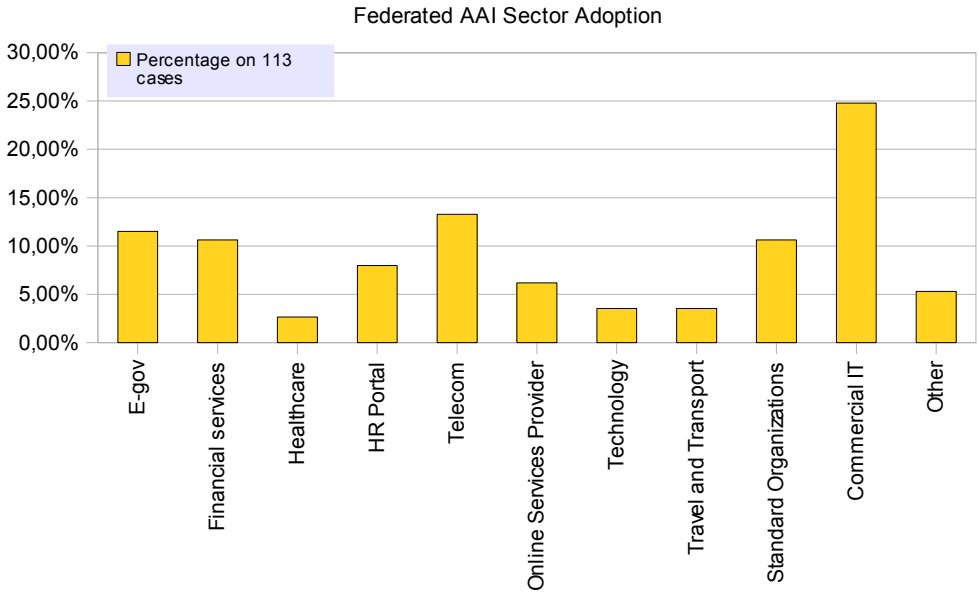

Figure 16 *Liberty Alliance application: sector view (Nov 2006).*

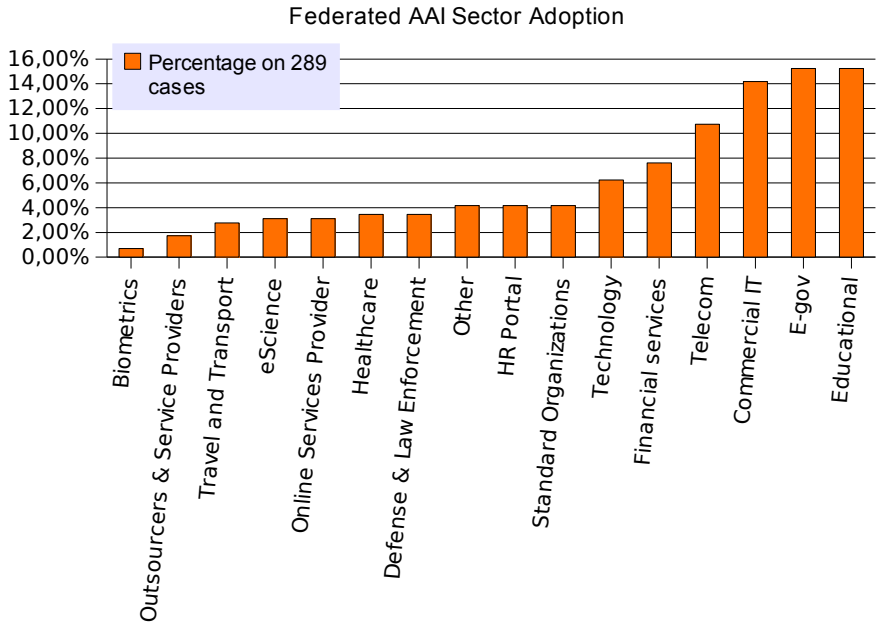

Figure 17 *Liberty Alliance application: sector view (Ago 2007).*

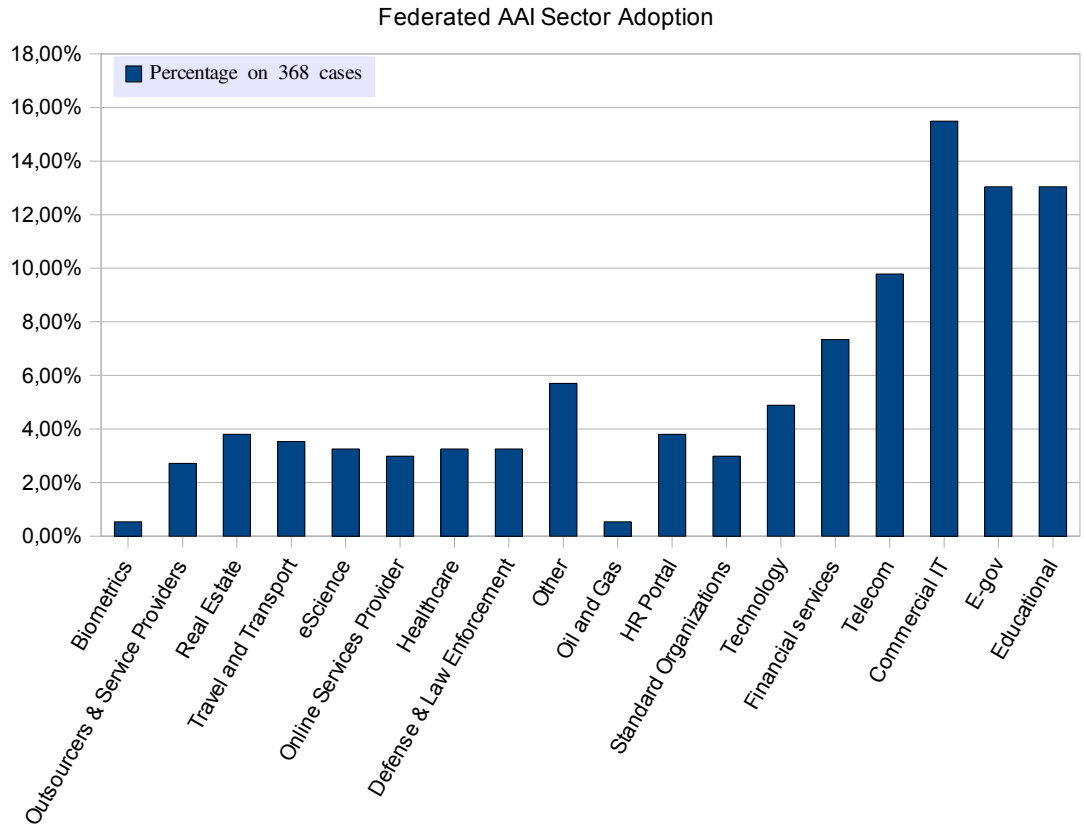

Figure 18 *Liberty Alliance application: sector view (Jun 2008).*

Da una prima analisi si evince, oltre ad un aumento dei casi di adozione, un aumento dei contesti in cui si è deciso di utilizzare il sistema Federato. Nella rilevazione del 2007 rispetto a quella del 2006 compaiono 4 settori in più rispetto ai precedenti: biometric, outsourcer & service provider, eScience, Defence & Law Enforcement, Educational. Mentre dal 2007 al 2008 si annoverano altri due settori: Real Estate, Oil & Gas.

Il grafico seguente illustra l'andamento di crescita del numero dei casi nei tre intervalli di tempo in cui si è effettuata la rilevazione.

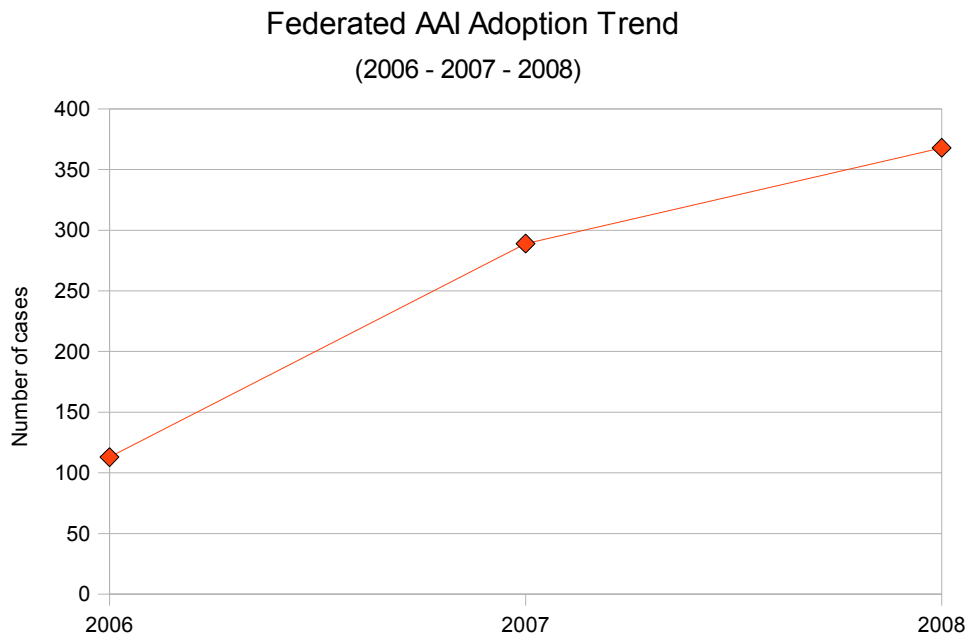

Figure 19 *Liberty Alliance application: adoption trend (2006 – 2007 - 2008).*

Si può osservare l'adozione di questo sistema segue un andamento crescente: si passa da 113 casi nel 2006 a 289 nel 2007, sino ad arrivare a 368 nel 2008.

Bisogna tenere presente che i dati analizzati sono solo quelli forniti dal sito del progetto Liberty Alliance, il quale è considerato uno standard di riferimento a cui si ispirano le varie soluzioni software che implementano un sistema federato per la gestione delle identità. I dati analizzati ogni anno non sono da considerarsi effettivamente implementati nello stesso ma possono a volte riferirsi ad un periodo precedente, Tale discrepanza dipende dall'intervallo di tempo che intercorre tra l'adozione e la realizzazione della documentazione da fornire a Liberty Alliance e la relativa notifica.

Nel paragrafo seguente si è cercato di analizzare una serie di casi per comprendere meglio la motivazione che porta all'adozione di tale sistema, cercando di distinguere i benefici tangibili (riduzione dei costi di gestione, aumento delle performance dei processi) e intangibili (come fiducia, sicurezza, privacy, usabilità) che ne scaturiscono.

3. Distribuzione settoriale dei casi di adozione dello standard Liberty.

Da un punto di vista qualitativo si è ritenuto analizzare nel dettaglio alcuni casi, selezionandoli tra i settori in cui i sistemi federati sono maggiormente diffusi, considerando 5 nel contesto educational, 7 nel contesto e-Gov e 11 nel contesto dell'e-Service B2B e B2C (in cui rientrano i settori Telecom, Commercial IT, Financial services, Tecnology e Standard organizations).

Inoltre sono stati selezionati 2 nel contesto sanitario in quanto, pur non essendoci una notevole diffusione (circa il 3,5%), la privacy e la sicurezza, affiancate all'efficienza del sistema informativo, ricoprono un ruolo particolarmente rilevante. Di seguito è fornito un sunto delle caratteristiche dei 25 casi considerati.

Contesto e-Health

In questo contesto sono stati analizzati i casi Catalan Health Service E-Prescription Project (Spagna) e US HIMSS (US). In entrambi vi è alla base la necessità di migliorare le performance dei processi legati all'interazione e allo scambio di dati tra i diversi sistemi informativi sanitari. Nel caso spagnolo, tramite l'utilizzo di un sistema federato, si vuole ottenere una più facile interazione tra medici, ospedali, farmacisti e sistema sanitario catalano al fine di migliorare e tracciare tutto ciò che

riguarda la gestione delle prescrizioni mediche. Nel secondo caso invece il focus è posto sull'efficienza del reperimento delle informazioni relative al paziente, spesso distribuite tra sistemi sanitari diversi. Nel primo caso l'enfasi è posta sul miglioramento dei processi di gestione delle prescrizioni, nel secondo sulla rapidità di ottenere le informazioni neccessarie relative ad un paziente (es. allergie a farmaci) la cui salute è in condizioni critiche.

Il comune denominatore in entrambi i casi è la necessità di permettere il trasferimento efficiente delle informazioni in modo sicuro salvaguardando l'integrità e la privacy del paziente, secondo lo standard HIPAA.

La soluzione di adottare in entrambi i casi un sistema federato permette la creazione di un circolo di fiducia tra i diversi sistemi al cui interno le informazioni sono scambiate rispettando tutti i criteri necessari di sicurezza e privacy, come conseguenza indotta si ha un aumento delle performance dei processi ed una riduzione dei costi legati alla gestione delle identità.

Contesto Educativo

In questo contesto sono stati analizzati i casi: EduMart (Giappone), SECURe (LSE - UK), Nilde (CNR Italia), EduTech (distretti scolatstici dello stato di New York) e SWITCH (università svizzere).

Tutti e cinque i casi hanno uno scopo comune: creare una federazione tra distretti scolastici, università e/o e-Library in modo da migliorare lo scambio di documentazione all'interno della federazione e allo stesso tempo snellire la gestione delle identità legate alle utenze, aumentando indirettamente il livello di sicurezza e privacy. Inoltre l'utilizzo di un sistema federato permette anche un miglior controllo

delle utenze e dei loro profili utilizzando un unico IdP all'interno dello stesso distretto scolastico o Ateneo (es. LSE) unificando così il processo di autenticazione per i vari servizi (email, e-library, accesso a workstation, ecc.) incrementandone il grado di usabilità.

Contesto e-Gov

In questo contesto sono stati analizzati i casi: Entr'ouvert (Francia), "Mon Service Public" (Francia), Finland eGov, Denmark eGov, NorthEast England eGov, eGov in UK, Ministero dei trasporti italiano.

I casi francesi offrono al cittadino la possibilità di poter accedere a diversi servizi tramite un unico identificativo, mirando ad una autenticazione sicura e rispettosa della privacy. Nel primo caso si tratta di un progetto che permette al cittadino di richiedere certificati e in futuro anche di poter votare; nel secondo caso si tratta di un servizio più complesso, basato su un portale che permette al cittadino, oltre di personalizzare la propria homepage, di fruire di una più ampia gamma di servizi, come pagare le tasse, modificare alcuni dati fiscali, richiedere certificati.

Il caso finlandese è simile ai due casi francesi. Differente invece è il caso danese, nel quale si cerca di riorganizzare i servizi di eGov già presenti, utilizzando un approccio decentralizzato per permettere l'interazione di differenti standard per la gestione delle autenticazioni e autorizzazioni dei cittadini. In particolare è prevista una federazione formata da sotto federazioni differenziate in base alla tipologia di servizio.

Il caso NorthEast England si pone come obiettivo inizialmente di creare una struttura federata per i servizi di eGov, successivamente per permettere l'interazione anche con servizi bancari a lungo termine con servizi sanitari ed educativi.

Nel caso eGov UK è stato adottato un sistema federato in quanto la gestione centralizzata esistente ha mostrato forti limitazioni con l'aumentare dei servizi offerti e del numero delle utenze.

Infine il caso del ministero dei trasporti italiano riguarda la realizzazione di un portale (SP e IdP) che da la possibilità all'utente di accedere ai propri dati presenti in motorizzazione (patente, informazioni sul veicolo, ecc.) e di effettuare on-line il pagamento delle pratiche automobilistiche attraverso posteitaliane (SP).

I casi menzionati hanno, oltre al miglioramento delle performance nell'erogazione dei servizi offerti, come punti critici la sicurezza e la privacy durante il trasferimento delle informazioni soprattutto nel caso dell'e-voting e dei pagamenti on-line.

Contesto e-Service

In questo contesto sono stati analizzati i casi: AOL – D-Link, BIPAC, Bluewin, Ebiz.mobility, General Motors, HP, Intel, Neustar, NTT – JAL, T-com, Telefonica Moviles España.

Mentre per i casi visti finora nei diversi contesti vi era una omogeneità nelle motivazioni, sicurezza e privacy per eGov ed eHealth e miglioramento dei servizi erogati potenziando l'interoperabilità per il contesto educational, per questi casi si è notato un più alto grado di eterogeneità legata soprattutto alle motivazioni che hanno spinto all'utilizzo di un sistema federato e alla creazione di una federazione o circolo di fiducia. In base all'analisi fatta è stato possibile creare una tabella in cui collocare gli 11 casi, evidenziando la tipologia delle relazioni (B2B, B2C o entrambi), e l'ambito di utilizzo (outsorcing - semplificazione dell'accesso a servizi interni all’organizzazione - interazione e collaborazione tra società partner).

Casi e descrizione	B2B	B2C	Outsourcing	Servizi interni	Collaborazione
AOL – D-Link: Semplificare l'erogazione di servizi multimediali di AOL (es.: Radio@AOL service) ai propri utenti che utilizzano apparati D-link (es.: D-Link Wireless Network Media Players)		X			X
Telefonica Moviles España: Poter fornire una più vasta gamma di servizi (in outsourcing) garantendo la privacy dei propri clienti, riducendo al contempo il mobile spam, utilizzando uno pseudonimo anzichè del numero di telefono del cliente richiedente		X	X		
T-com: offrire ai clienti e ai partners un accesso facile, veloce e sicuro ai propri servizi creando un circolo di fiducia formato da T-com e da business partners.		X			X
NTT – JAL: Migliorare il sistema di gestione delle trasferte dei dipendenti, esternalizzando tutto il processo a JAL on line (compagnia aerea giapponese)	X		X		
Neustar: Passare da un traffico dei documenti cartaceo, che comporta costi materiali e tempo, all'invio telematico, creando un circolo di fiducia tra i partner	X				X
Intel: razionalizzare l'accesso degli impiegati a diversi servizi dati in outsourcing	X		X		
HP: migliorare l'interazione di clienti, impiegati e partner; ridurre i costi; sviluppare nuovi business	X	X	X	X	X
General Motors: migliorare il controllo e la facilità d'uso dei servizi della propria rete sia da parte degli utenti che dei dipendenti	X	X		X	
Ebiz.mobility: fornire una soluzione per rendere più sicuro e flessibile (possibilità di micropagamenti) il pagamento on-line al fine di incoraggiare il commercio via rete (PC e mobile device)	X	X			X
BIPAC: semplificare l'accesso alle informazioni.	X	X			X

Casi e descrizione	B2B	B2C	Outsourcing	Servizi interni	Collaborazione
Bluewin: semplificare il riconoscimento del cliente da parte dell'ISP Bluewin permettendo l'accesso in SSO a tutti i service provider all'interno del circolo di fiducia		X			X

Tabella 4. *Casi di utilizzo di un sistema federato nel contesto eService.*

Per tutti i casi presenti in tabella la fiducia ricopre un ruolo fondamentale. Per i casi B2C la fiducia riposta dagli utenti finali nel sistema con cui interagiscono diventa anche un punto a favore per i SP facenti parte del circle of trust, sia per quanto riguarda le operazioni di pagamenti on-line (es. Ebiz.mobility) sia per quanto riguarda le informazioni legate alle loro identità (es. Telefonica Moviles España). Per i casi B2B l'adozione di un sistema federato diminuisce la possibilità di comportamenti opportunistici da parte dei partner, favorendo la creazione del clima di fiducia (Ciborra 1989). In oltre l'utilizzo di un sistema di questo tipo permette di diminuire notevolmente i costi di gestione delle identità e favorire le collaborazioni con nuovi partner che desiderino entrare a far parte della federazione, creando possibili nuove opportunità di business.

4. Conclusioni

Da quanto descritto sinora le motivazioni che portano ad adottare un sistema federato per la gestione delle autenticazioni e autorizzazioni possono riguardare aspetti tangibili, volendo agire direttamente sui costi di gestione, abbassandoli, e sui processi di interazione, migliorandoli, o aspetti intangibili, privilegiando la privacy dei dati dell'utente e la sicurezza nelle transazioni, contribuendo così ad accrescere il grado di fiducia che gli utenti (o partner) ripongono nel sistema.

Nella figura seguente sono rappresentate le motivazioni dei casi presi in esame, raggruppati per settore.

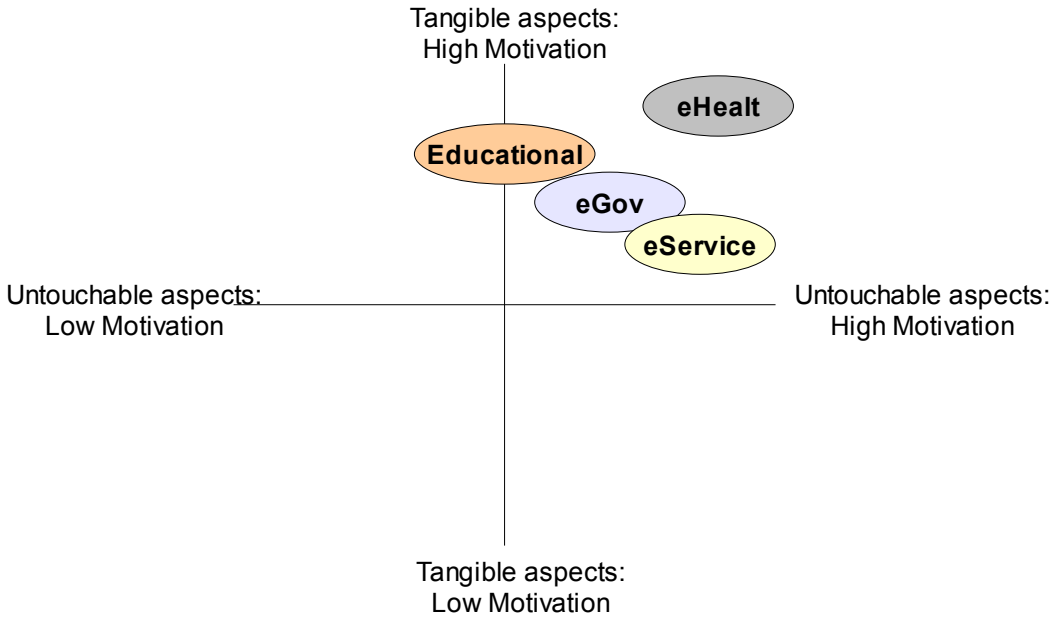

Figure 20 *Adoption motivation: Tangible vs Untouchable aspects*

In genere dall'analisi dei casi considerati, qualunque sia la motivazione, l'adozione di un sistema federato per la gestione delle autenticazioni e autorizzazioni influenza in maniera diretta o indotta la fiducia ai vari livelli, rafforzando quella istituzionale o influenzando la fiducia personale, considerando che spesso gli utenti inconsciamente tendono a considerare il sistema o l'artefatto tecnologico come un "social actor", applicando così regole sociali durante l'interazione (Reeves and Nass 1996), quindi se ripongono fiducia nel sistema (gestione delle informazioni personali – privacy – e sicurezza) saranno maggiormente propensi all'interazione (technological trust).

5. Bibliografia

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Intial Test. Journal of Management Information Systems, 19 (1), 211-242

C. Ciborra (1989) “Tecnologie di Coordinamento” Franco Angeli, Milano, 142-145

Elden, M. and Chisholm, R.F. "Emerging Varieties of Action Research: Introduction to the Special Issue," *Human Relations* (46:2), 1993, pp. 121-142.

Gable, G., "Integrating Case Study and Survey Research Methods: An Example in Information Systems," European Journal of Information Systems, (3:2), 1994, pp. 112-126.

Kaplan, B. and Duchon, D. "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," MIS Quarterly (12:4) 1988, pp. 571-587.

Lee, A. S. "Integrating Positivist and Interpretive Approaches to Organizational Research," Organization Science, (2), 1991, pp. 342-365.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. (1995). An Integrative Model of Organizational Trust. Academy of Management Review, 20 (3), 709-734.

Mingers, J. "Combining IS Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3), 2001, pp. 240-259.

Ragin, C. C., *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*, University of California Press, Berkeley and London, 1987.

Reeves, B. and Nass, C. (1996). The Media Equation: How People Treat Computers, Television and New Media like Real People and Places. Cambridge University Press, New York.

Walsham, G. *Interpreting Information Systems in Organizations*, Wiley, Chichester, 1993.

6. Risorse Web consultate per i casi

AOL–D-Link,
http://www.projectliberty.org/liberty/content/download/409/2790/file/AOL_Use_Case_Study.pdf

BIPAC,
http://www.projectliberty.org/liberty/content/download/410/2793/file/bipac_casestudy.pdf

Bluewin,
http://www.projectliberty.org/liberty/content/download/412/2799/file/bluewin_casestudy_web.pdf

Catalan Health Service E-Prescription Project,
http://www.projectliberty.org/liberty/content/download/2827/18948/file/Alamillo%20CATCert%20-%20I%20Alamillo.pdf

Denmark eGov, http://www.oio.dk/arkitektur/brugerstyring/english

Ebiz.mobility, http://www.projectliberty.org/liberty/content/download/414/2805/file/eBIZ_casestudyFINAL.pdf

EduMart,
http://www.projectliberty.org/liberty/content/download/415/2808/file/EduMart_Use_Case_Study.pdf

EduTech,
http://www.projectliberty.org/liberty/content/download/2458/15859/file/EduTech-CaseStudy.pdf

eGov in UK,
http://www.projectliberty.org/liberty/content/download/2460/15865/file/UK-CaseStudy.pdf
Entr'ouvert, http://www.projectliberty.org/liberty/content/download/2214/14718/file/Entr'ouvertFINAL.pdf
Finland eGov, http://www.projectliberty.org/liberty/content/download/417/2814/file/Finland_casestudyFINAL.pdf
General Motors, http://www.eweek.com/article2/0,1759,1768255,00.asp
HP, http://www.projectliberty.org/liberty/content/download/2428/15723/file/HP-CaseStudyNov06.pdf
Intel,
http://www.projectliberty.org/liberty/content/download/419/2820/file/Intel_casestudyFINAL.pdf
Mon Service Public,
http://www.projectliberty.org/liberty/content/download/685/5107/file/Tokyo_2004_ADAE.pdf
Ministero dei trasporti italiano,
http://blogs.sun.com/superpat/entry/federation_italian_style
Neustar,
http://www.projectliberty.org/liberty/content/download/420/2823/file/Neustar_Use_Case_Study.pdf
Nilde, http://nilde.bo.cnr.it/
NorthEast England eGov,
http://www.projectliberty.org/liberty/content/download/809/5784/file/sunderland_gov.pdf

NTT–JAL,
http://www.projectliberty.org/liberty/content/download/421/2826/file/ntt_casestudy_web.pdf

SECURe, http://www.angel.ac.uk/SECURe/

SWITCH, http://www.switch.ch/it/aai/

T-com, http://www.projectliberty.org/liberty/content/download/2459/15862/file/T-Com-CaseStudy.pdf

Telefonica Moviles España, http://www.projectliberty.org/liberty/content/download/422/2829/file/telefonica_casestudy1_FINAL.pdf

US HIMSS,
http://www.projectliberty.org/liberty/content/download/461/2946/file/HIMSS_Liberty_2006_handout.pdf

CONCLUSIONI E SVILUPPI FUTURI

1. Conclusioni

Nel primo capitolo si sono fornite diverse definizioni di fiducia ed un modello concettuale utilizzato per fornire una possibile visione del suo ruolo all'interno delle relazioni elettroniche, distinguendo tre tipologie di fiducia: personale (o sociale), istituzionale (o organizzativa) e tecnologica.

Si è deciso di utilizzare il modello TFI (technical, forma, informal model) per guardare alle relazioni elettroniche come scambio di informazioni, regolato sui tre livelli definiti dal modello.

Si è proposto un modello integrato di visione delle relazioni collegando le tre tipologie di fiducia ai tre livelli (informale, formale e tecnologico).

Soffermandosi sul livello tecnologico e sul concetto di fiducia nella tecnologia, partendo dal fatto che sono i meccanismi legati alla sicurezza quelli che hanno maggiore influenza, si è fornita una loro tassonomia formata da tre classi (effettuando un confronto con un altra proposta in letteratura): accesso, trasferimento e gestione delle informazioni.

Ci si è soffermati sui meccanismi abilitanti la fiducia appartenenti alla prima classe e si è deciso di analizzare il sistema federato per la gestione delle autenticazioni e autorizzazioni, fornendo una sua descrizione di sintesi.

Nel secondo capitolo si è proposta un'analisi concettuale dell'utilizzo di questo sistema all'interno del modello delle virtual organization, eseguendo un confronto tra il framework ECB ed il concetto di circolo di fiducia (circle of trust o federazione)

Nel terzo capitolo si è descritta l'adozione del sistema federato all'interno di un progetto europeo (LD-CAST). Il quale mira a supportare la cooperazione transfrontaliera tra le camere di commercio (CC), al fine di sostenere lo sviluppo delle iniziative delle società private dei paesi partner. In questo contesto I meccanismi con cui vengono scambiate le informazioni ricoprono un'importanza rilevante (fiducia e privacy), portando ad optare per l'utilizzo di un sistema federato (dove ogni camera di commercio svolge il ruolo di IdP) e rinunciando all'utilizzo di un sistema centralizzato inizialmente proposto.

In fine, nel quarto capitolo sono stati proposti i risultati dell'analisi dei casi di adozione del sistema federato, la cui documentazione è presente sul sito Liberty Alliance (uno dei principali standard di riferimento per le AAI federate), individuando le motivazioni che hanno portato all'adozione di questo particolare tipo di sistema nei diversi settori di appartenenza (e-Gov, Educational, e-Health, e-Service). Il risultato ha portato anche alla individuazione delle possibili motivazioni che in genere possono portare all'adozione, menzionati di seguito:

- aspetti legali,
- miglioramento dei processi di comunicazione:
  - interni (tra unita organizzative),
  - esterni (relazioni inter-organizzative),
- aumento della fiducia,
- opportunità di business e/o vantaggio competitivo[13] (facilità di adesione a circoli di fiducia).

[13]SCHLAEGER C. e PERNUL G.. Authentication and Authorisation Infrastructures in b2c e-Commerce. Lecture notes in computer science. Springer-Verlag Berlin Heidelberg 2005, pag 306-315

2. Sviluppi futuri

La ricerca ha portato alla definizione di un modello concettuale con cui guardare il rapporto tra fiducia e tecnologia nelle relazioni elettroniche, definendo una tassonomia per classificare i meccanismi di sicurezza, quali maggiormente influenti.

Si è deciso di guardare ai meccanismi appartenenti alla prima classe (accesso alle informazioni) ed in particolare alle AAI federate.

Gli step successivi saranno volti ad analizzare l'utilizzo di questo sistema combinato con il sistema biometrico di identificazione dell'utente (sviluppato dall'università di Regensburg[14]), e le relative ripercussioni sugli aspetti legati alla fiducia.

[14]Olden M., Za S., "Federated AAIs with biometric authentication: Increasing security and trust in organizational relationships" itAIS 2008, V Conference. of Italian Chapter of AIS, Dec. 13-14, 2008, Paris, France