Fiducia e tecnologia nelle relazioni elettroniche inter-organizzative

1. Introduzione

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.

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 tre casi (di cui due teorici) 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.

2.1 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.

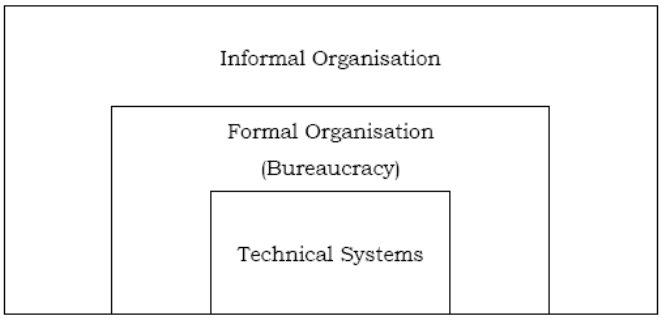

Figura 1. *The embedding of computer systems in the formal and informal organisation (Stamper et al, 2000)*

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.

2.2 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).

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 di seguito illustra la relazione tra individuo ed organizzazione scomposta nei tre livelli.

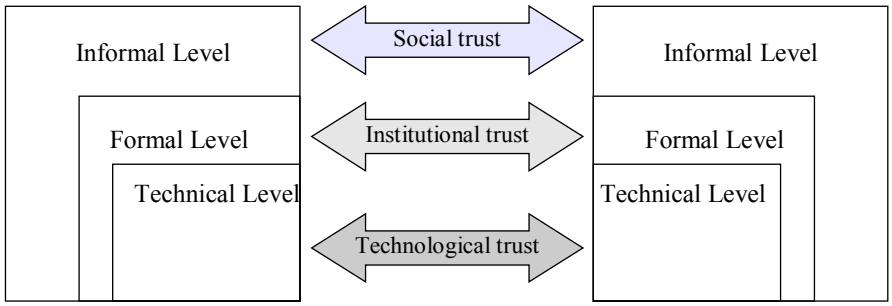

Figura 2. *The relationships between the three trust concepts and the TFI levels*

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 opportunistici da parte del partner. È questo lo scenario tipico delle relazioni basate completamente sull'IT.

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 basandosi 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

Una volta identificate queste classi, per questo lavoro 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.

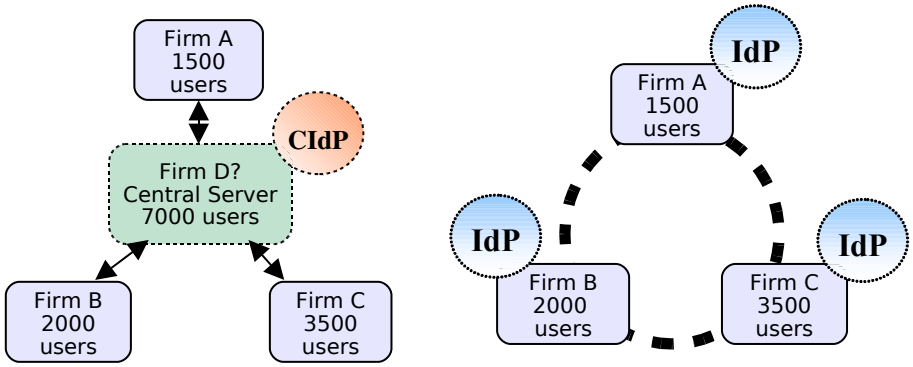

Figura 3. AAI: centralized system vs federated system

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.

	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	Complessa	Fattibile

Tabella 1. *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..

Per i casi riportati in questo lavoro si fa riferimento a questo tipo di sistema, il quale verrà meglio descritto nel prossimo paragrafo.

3.1 I sistemi federati

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.

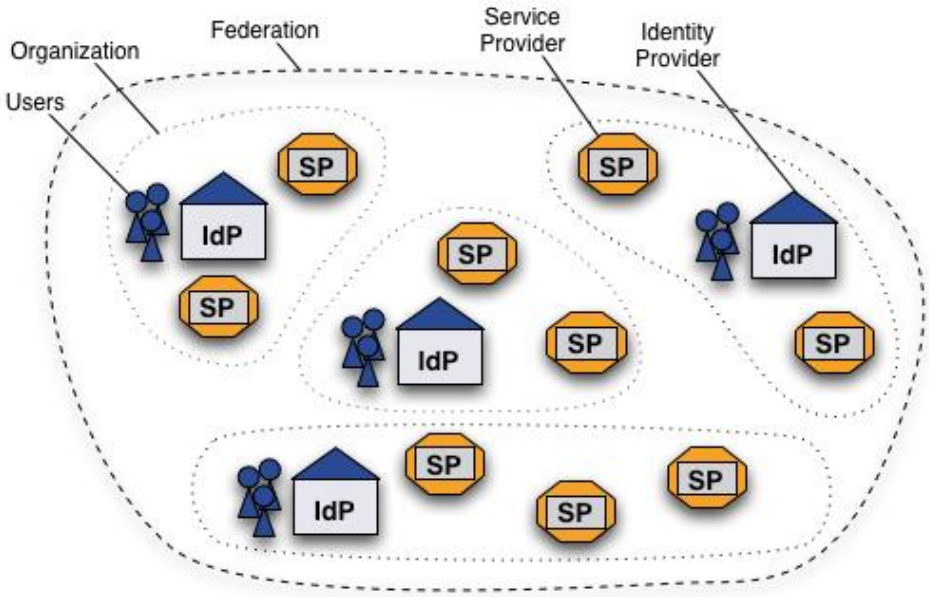

Figura 4. *Circe of trust.*

Nel momento in cui un utente accede al Circolo, il suo IdP crea un "handle" e lo invia al suo user agent (l'applicazione più comune è il web browser). Tale handle è affidato allo user agent fino al momento del logout ed è accettato da qualsiasi IdP o

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

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 non solo dagli accordi formali previsti dal Circolo stesso, ma anche dalla fiducia nel sistema utilizzato in quanto non comporta nessuna alterazione sulla gestione delle informazioni sulle identità (restano circoscritte all'interno del relativo IdP), permettendo un maggior controllo su chi ha accesso alle informazioni sensibili e su come e a chi vengono inviate.

4. Domanda di ricerca e struttura della tesi

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), questo lavoro presenta 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) sui casi menzionati.

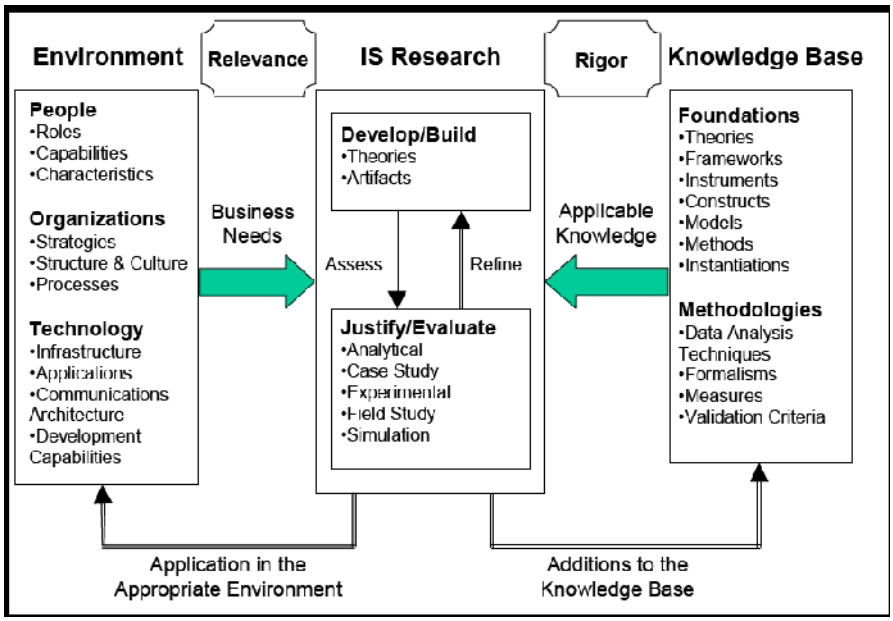

Figura 5. *Information Systems Research Framework (Hevner et al. 2004)*

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 tre soggetti (quali il broker, catalyst e enabler) e relativi utenti.

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 delle nazioni partner un servizio integrato relativo all'avvio di attività trans-nazionali.

Infine mostra i risultati di un analisi di 25 casi di adozione del sistema in questione distribuiti in quattro settori: e-Gov, Educational, e-Health ed e-Service. Da questa analisi si evince che 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

2 Il progetto LD-CAST 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.

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 è rappresentata la distribuzione delle motivazioni dei casi presi in esame, raggruppati per settore.

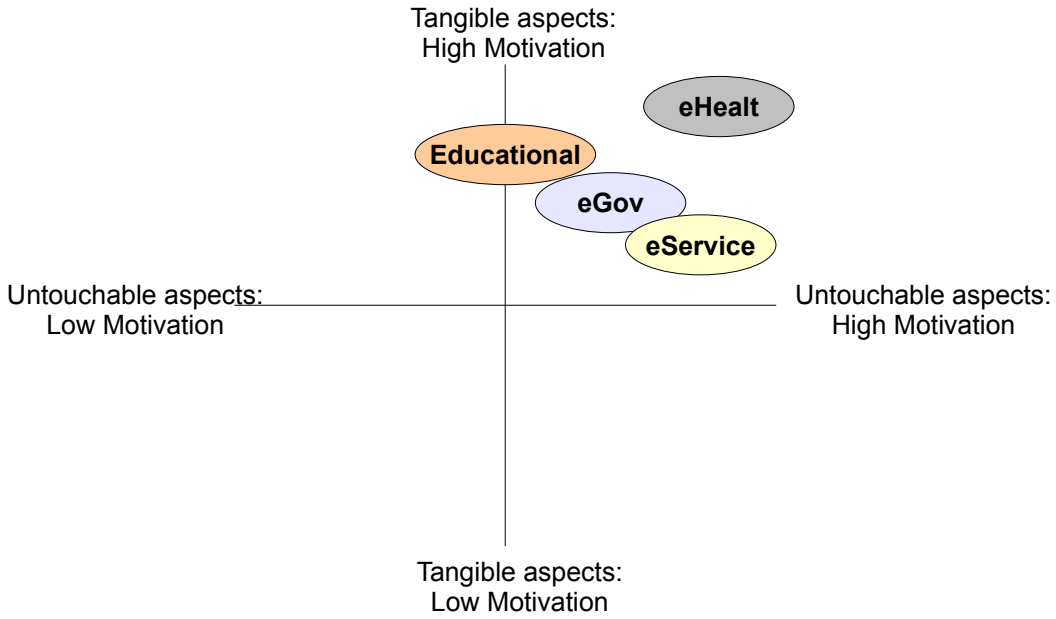

Figure 6 *Adoption motivation: Tangible vs Untouchable aspects*

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).

Gli sviluppi futuri di questo lavoro riguardano l'adozione del sistema federato combinato con il sistema di autenticazione biometrico. In questo scenario oltre al processo di autenticazione ed autorizzazione viene effettuato anche quello di identificazione dell'utente (chi fisicamente sta cercando di effettuare l'accesso), proponendo che un aumento delle misure di sicurezza porta un aumento del livello di fiducia nella tecnologia che si ripercuote ai livelli più alti.

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.

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., 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.