

UNIVERSITÀ DEGLI STUDI DI SALERNO  
DIPARTIMENTO DI INFORMATICA

---

DOTTORATO DI RICERCA IN INFORMATICA  
XIV CICLO - NUOVA SERIE



TESI DI DOTTORATO IN

# Augmenting the Internet with a Trust Ecosystem for inter pares interactions

*Candidate*

**Fernando Antonio PASCuccio**

*ID: 8880900109*

*Tutor*

**Chiar.mo Prof.  
Gennaro COSTAGLIOLA**

*Co-Tutor*

**Dott. Vittorio FUCCELLA**

**Coordinator:** Chiar.mo Prof. Gennaro COSTAGLIOLA

---

ANNO ACCADEMICO 2014/2015

I would like to dedicate this thesis to my wonderful kids:  
*“Never lose your intellectual curiosity”.*

## **Acknowledgements**

I am very grateful to my advisor Gennaro Costagliola for his patience, his collaboration, his guidance and his fundamental contributions to my research work. I would like to thank Vittorio Fucella for his fundamental contributions in my research and publication activity. I am thankful to my colleagues and friends Luchino and Arcangelo, with whom I shared my phd experience. I am very grateful for their precious attentions and for having helped me each moment I needed them. Finally, I thank my wife for her patience and her support.

## Abstract

The Internet is an extraordinary communications medium but it is not free from problems that are limiting its potential further development. In this dissertation we analyze and address some of the issues that make it an unsafe and unreliable place and we exhibit the most difficult issues that, as soon as possible, would deserve to be resolved such as: the uncertainty of the identities; the almost complete lack of privacy and of guarantees on the reliability of the counterparts (i.e., the lack of trust among people); the lack of control and ownership of the information regarding a person or a company; the lack of specific information about service providers; the exploitation of anonymity to perform malicious actions. These issues mainly arise from the very nature of the Internet which is a deregulated place where users have the possibility to act and communicate in total freedom while keeping the anonymity. However, these aspects should, in our opinion, be balanced with the protection of the fundamental users' rights.

The main goal of our research is to combine the positive aspects and the strengths of the Internet with the need to introduce environments or areas where users can enjoy greater mutual trust. To this aim, we proposed a solution to augment the Internet to make it a safer and more reliable place. Our proposal allows users to interact with higher security than at present and to have better guarantees on the respect for their rights and their needs. In other words, based on the above reasons, in this work our objective is the design of a comprehensive framework aimed at providing a trust area in the Internet that combines the online and offline world smoothly and seamlessly, including the best solutions in a single model. Our integrated and modular model is called **Trust Ecosystem** (TEco) where “ecosystem” means an environment where the entities (e.g., users and online services) preserve the system and comply with fixed rules, are proactive and responsive as each of



them, using a reward-punishment mechanism (feedback), contribute to the success of the system and, consequently, to their own benefit.

The TEco was built by integrating different innovative systems. It is a Internet-based area in which users: own a Trusted Digital Identity to authenticate keeping anonymity; establish Inter Pares Interactions based on contracted agreements and knowing each other's reputation; can be the owners of the information they produce and protect their privacy. The coexistence of these features makes the TEco a trust area. In fact, users can mutually trust, as they are all identifiable, their reputation is known and while interacting, they can bargain conditions with law effectiveness. Furthermore, depending on their needs and the demands of others, users can decide which information to disseminate, protecting their privacy or maintaining complete anonymity.

The TEco has been conceived without "upheavals" of the current Internet and for this reason the TEco can develop in parallel with it and, in any case, they can coexist. In fact, the users will not be forced to drastically change the way in which they normally use both Internet services and Web browsing.

In our view, to obtain a Trust Area there is the need of effective Trust and Reputation systems. Although new Trust, Reputation and Recommendation (TRR) models are continuously proposed in literature, they lack shared bases and goals. For this reason, in this work we pay special attention to the problems related to Trust and Reputation management that are among the most controversial issues of the Internet. So, we address trust and reputation in all their aspects and we define an innovative meta model to facilitate the definition and standardization of a generic TRR model. Following the meta model, researchers in the field will be able to define standard models, compare them with other models and reuse parts of them. A standardization is also needed to determine which properties should be present in a TRR model.

In accordance with the objectives we were seeking, following our meta model we have: defined a pre-standardized TRR model for e-commerce; identified the fundamental concepts and the main features that contribute to form trust and reputation in that domain; respected the dependence on the context/role of trust and reputation; aggregated only homogeneous trust information; listed and shown how to defend from the main malicious attacks.

Lastly, in this work, we also discuss the feasibility of the Trust Ecosystem, the compatibility with the current Internet and the things to do for putting it into practice. For this purpose, we show some scenarios that also highlight and make advantages and potentiality of the TEco fully understandable.

In the future, the TEco may also act as a “*field of comparison*” and facilitate scientific communication in the sector and, like a digital ecosystem, can play the role of a unification “*umbrella*” over significant, challenging and visionary computing approaches that emerge in parallel.

# Contents

<b>Contents</b>	<b>vi</b>
<b>List of Figures</b>	<b>viii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Aims and Objectives . . . . .	5
1.2 Outline . . . . .	7
<b>2 Research Context</b>	<b>8</b>
2.1 State of art . . . . .	9
<b>3 Trust Ecosystem</b>	<b>17</b>
3.1 Related Work . . . . .	18
3.2 Trusted Digital Identity . . . . .	19
3.3 Inter Pares Interaction . . . . .	22
3.4 Content Management Framework . . . . .	25
3.5 Discussion . . . . .	26
<b>4 Trust, Reputation and Recommendation Meta Model</b>	<b>29</b>
4.1 Related Work . . . . .	30
4.2 Definition of the TRR-Meta Model . . . . .	32
4.2.1 TRR Meta Model Part 1 - Basic principles . . . . .	34
4.2.2 TRR Meta Model Part 2 - Information Management . . . . .	35
4.3 A Pre-Standardized Trust and Reputation Model for E-Commerce	37
4.3.1 TRR Model for E-Commerce Part 1 - Basic principles . . . . .	37

---

4.3.2	TRR Model for E-Commerce Part 2 - Information Management . . . . .	43
<b>5</b>	<b>Scenarios of the Trust Ecosystem</b>	<b>47</b>
5.1	Scenario 1: TEco accreditation. . . . .	51
5.2	Scenario 2: Single Sign-On in the TEco . . . . .	54
5.3	Scenario 3: Management of IAEs . . . . .	56
5.4	Scenario 4: Web surfing . . . . .	58
5.5	Scenario 5: Negotiated Interaction Agreement . . . . .	62
5.6	Scenario 6: InterPares Interactions . . . . .	69
5.7	Scenario 7: TEco Inter Pares Interactions with Banks and Institutions . . . . .	73
<b>6</b>	<b>Achievements and Future Research</b>	<b>75</b>
	<b>References</b>	<b>79</b>
	<b>Acronyms</b>	<b>94</b>
	<b>Index</b>	<b>95</b>

# List of Figures

3.1	Interaction between entities in the TEco. . . . .	23
4.1	TRR Meta Model - Main Components of Information Management.	33
4.2	Categorization of the information according to: context/role, main feature and main feature values. . . . .	40
5.1	Main interface of the TEco-Console. . . . .	48
5.2	TEco key. . . . .	49
5.3	Selection of the IAE and the ICR for a TEco Inter Pares Interaction.	50
5.4	Browser with TEco interactions' icons. . . . .	50
5.5	Information about an IAE in the TEco. . . . .	52
5.6	TEco accreditation sequence. . . . .	53
5.7	TEco accreditation request. . . . .	55
5.8	TEco Single Sign-on . . . . .	56
5.9	Management of IAEs with the TEco-Console. . . . .	57
5.10	Creation of a new Internet Alter Ego. . . . .	58
5.11	An Alter Ego and an Agreement to surf the Web. . . . .	59
5.12	An Alter Ego and an Agreement of a website. . . . .	60
5.13	Browser with the TEco's icon. . . . .	60
5.14	Selecting an IAE. . . . .	61
5.15	Browser with Bob's IAE icon. . . . .	61
5.16	Browser with entities' icons. . . . .	61
5.17	Browser with entities' icons and Inter Pares interaction's icon. . .	62
5.18	Alter Ego of Teacher Mario and his agreement. . . . .	63
5.19	Alice's IAE and her agreement. . . . .	64

---

5.20	Teacher's advertisement. . . . .	64
5.21	Teacher's website. . . . .	65
5.22	Notification of a TEco interaction request. . . . .	66
5.23	Details of the notification. . . . .	67
5.24	Notification of a TEco interaction acceptance with details. . . . .	68
5.25	Bob's IAE named <i>Amazon-AE</i> . . . . .	69
5.26	Duplication of an IAE. . . . .	70
5.27	Interaction feedback. . . . .	71
5.28	Bob's IAE named <i>TrustworthyEcommerce-AE</i> . . . . .	72

# Chapter 1

## Introduction

The Internet has been one of the greatest revolutions that humanity has ever known. The possibility to communicate in real time, the birth of the Web and the freedom of initiative of users greatly fostered its development. In addition, the progressive reduction of access costs (of both devices and connection to the telephone network), further contributed to facilitate mass participation.

The diffusion of social networks and the introduction of increasingly sophisticated smartphones also allowed an increase of the time spent online so that today, in many countries, almost all people are always connected.

Despite its enormous success and indisputable usefulness, the current Internet is not exempt from problems. In fact, in the fervent research on the Future Internet several authors emphasize the crisis of the current Internet and its services [86]. It is undeniable that the Internet has several crucial weaknesses that are restricting its potential further development [105, 107, 121]. Some of these weaknesses are the uncertainty of the identities, the almost complete lack of privacy and of guarantees on the reliability of the counterparts (i.e. the lack of trust among people), the lack of specific information about service providers (e.g., reliability, quality, punctuality, etc. i.e, their reputation), the lack of control and ownership of their own information, the exploitation of anonymity to perform malicious actions [44, 54], and so on.

In the following, we detail some of these issues by categorizing them in 4 macro-areas:

- *Privacy and data control;*
- *Cybercrimes;*
- *Accreditation;*
- *Security and Reliability.*

The aforementioned problems afflict the Internet and reflect badly upon the user making her/him insecure and less incline to trust online services and other users. For these reasons, in our opinion, they should be addressed and resolved. This is exactly the objective of our research work.

**Privacy and data control.** The widespread distribution of social networks, which soon passed from being used by a small group of people to a crowd globally interconnected, raised a number of issues related to privacy. Initially, social networks were used to connect friends and relatives or small groups of people with a high degree of confidence with little or no need of privacy [53]. Today they mostly connect unknown people and, unfortunately, privacy protection is still very weak. Since the information on social networks is perpetually and globally accessible, the problem is particularly magnified. Despite the actions taken to stem the countless violations of privacy, the issue is still open.

The lack of control of the data presents another critical aspect. In fact, a user does not have complete control of the information concerning her/him and, if s/he wishes to delete even a single part of it, s/he will never be sure that it will be permanently deleted from the Web. For example, it often happens that when a post on a blog or on a forum is inserted, others extrapolate a part or they fully copy the content without authorization using it for their own purposes and attributing its authorship to themselves implicitly. In these cases and, in general, for all types of digital content (video, picture, music, text, etc.) the real authors can not claim authorship.

In addition, users cannot keep trace of the use of their digital contents neither they can impose any limitations on use. In practice, there is no way to prevent contents from being reused in other contexts (e.g. articles on a blog) nor to delete them permanently from the Internet, namely to gain the respect of “*the right to be forgotten*”. Indeed the European Union issued a directive in 2014 stating “*the*



*right to be forgotten*". Following it, Google implemented the "*Request Removal from Google*" that should permanently remove the information associated with the requesting user.

**Cybercrimes.** The privacy violation, also brings with it a series of further subtle but pernicious problems. The most insidious is definitely the "*digital identity theft*", one of the fastest growing crimes in recent years. The digital identity theft is put in place to achieve economic purposes (theft of credit cards, home banking, etc.), to create inconvenience and reputational damage to third parties (e.g. defamation, unfair competition) and to have various benefits (e.g. ghosting, documents fraud). Children are certainly the most exposed and vulnerable to cybercrime because they are always connected to the Internet without control and they naively share many personal data, smoothly integrating their offline and online lives. The European Union has highlighted the potential risks to children and denounced the rise of "*cybercrime*" ranging from child abuse to identity theft as well as their greater exposure with respect to "*illegal*", "*age inappropriate content*", "*poor contact*" and "*inappropriate behavior*" [30].

Another face of danger crimes committed through Internet is framed under the name of "*cyberbullying*". According to the EU Commission, "*Cyberbullying is repeated verbal or psychological harassment carried out by an individual or group against others. It can take many forms: mockery, insults, threats, rumours, gossip, "happy slapping", disagreeable comments or slander. Interactive online services (e-mail, chat rooms, instant messaging) and mobile phones have given bullies new opportunities and ways in which they can abuse their victims.*" [28]. Usually they come to the fore only the most tragic cases of cyberbullying but also those that remain in the shadows are just as devastating because, as it is well known, it has long term consequences on the victims [3, 21]. The European Commission also highlights that the measures taken so far by the member States have been on the whole inadequate. Therefore it suggests to increase efforts to make the Internet a safer place and makes this issue a priority of the Digital Agenda for Europe [29].

**Accreditation.** Another strongly felt need is that of being able to perform a single "*accreditation*" and be able to request services to different providers without the need to perform, from time to time, the login at each one of them. Generally, organizations (i.e. companies, academics, online fora, etc.) authenticate users and

grant them roles through proprietary authentication mechanisms and the users are forced to identify themselves to each provider using identification methodologies imposed by them. This mechanism only makes the online experience worse and does not guarantee that data are treated in compliance with privacy.

In addition, the use of the same credentials to access all the accounts constitutes a security risk. As an example, a service provider may use the passwords of its customers to access all their other accounts. So far several solutions have been implemented, known as Single Sign-on (SSO) only in a few specific areas or restricted to the same organization. At present, there is no possibility of a global accreditation for all Internet services. It is known that more and more providers accept the accounts of Facebook and Google+ for access to their online services. In fact, this practice is imposing as a sort of global Single Sign-on. However, it is a kind of a proprietary Single Sign-on mechanism and it goes in contradiction with the “open” nature of the Internet. Therefore, it would be desirable the introduction of non-proprietary solutions, exactly as it was in the case of the basic Internet protocols.

**Security and Reliability.** The analysis of the problems of the Internet can not be separated from those relating to the security of systems and the reliability of the parties with which it interacts in the Internet. Normally a system is considered safe when it is able to ensure that any unauthorized access to resources will be locked [35, 58]. In general, security mechanisms allow to protect services and resources by restricting access only to accredited users and to provide protection from malicious third parties. However, in many situations users need to protect themselves from those who offer resources and services, and so the problem is inverted. In this case the user needs to identify the provider that is giving the service and its reliability, that is the quality of the products and services offered. This is similar to the case when, visiting a foreign country, we need to have medical assistance and we want to know if the person to whom we are addressing is really a doctor (identification) and if s/he is a good doctor.

The first necessity is resolved by using traditional security mechanisms which are able to guarantee, through the accreditation systems, that each entity is recognized and identified, that is, it is exactly what it has declared to be. As regards the second necessity, the classical mechanisms are totally ineffective because they do

not provide any information on the “skills” of the doctor. In this case, a user needs to know the opinion that others have of that doctor, that is his/her reputation.

In the case of online services, the problem is further amplified by multiple factors. First of all, the biggest problem is originated by the extreme ease, both technical and economic, with which anyone can become a service provider at any moment, bragging skills and qualities. Moreover, there is little information about service providers (e.g. reliability), most of which is self-declared by the provider. It is not even possible to request guarantees and/or data about them and, however, there is no specific information even on the requested service (e.g., quality). Obviously, this is not referred to the case where the supplier is known a priori or it has established itself on the market for a long time (e.g., Amazon, eBay etc.).

## 1.1 Aims and Objectives

So far, we have outlined the main reasons why the Internet is, de facto, a virtual jungle where less experienced people proceed through trial and error or, as it often happens, simply they do not use the online services except those already well-established. Indeed, if compared to the number of users connected to the Internet, online services appear to be poorly used and new and more sophisticated services are hampered. The problems so far described arise mainly from the “open” nature of the Internet and the ability to act and to communicate in total freedom also maintaining anonymity. However, these positive aspects should be balanced by the protection of the fundamental rights of users.

It grows more and more the need to have environments or areas where users can enjoy greater trust and more guarantees on respect for their rights and needs.

In recent years many studies have focused on the development of new protocols and methodologies to allow unambiguous identification of the user, the ability to keep anonymity, to protect privacy and to authenticate, just for one time, to access many services (*Single Sign-On*) [18, 115]. However, the aforementioned issues were almost always addressed individually and, in any case, not all together in a single model.

Based on the above reasons, in this work our objective was the design of a com-

prehensive framework aimed at providing a trust area in the Internet that combines the online and offline world smoothly and seamlessly, including the best solutions, in a single model. Our integrated and modular model is called **Trust Ecosystem** (TEco). Here, *ecosystem* means “*a loosely coupled, domain clustered, collaborative environment where each species conserves the environment, is proactive and responsive for its own benefits*” [20, 24, 127]. In our case, species are the entities (e.g., users and online services) which preserve the environment and comply with fixed rules, are proactive and responsive as each of them, using a reward-punishment mechanism (feedback), contribute to the success of the system and, consequently, to their own benefit. Digital ecosystems, as emphasized in [89], “*can play the role of a unification ‘umbrella’ over significant, challenging and visionary computing approaches that emerge in parallel*”. In this sense the TEco will also act as a “*field of comparison*” to facilitate scientific communication in the sector.

One of the main strengths of this model is that it does not require an “*upheaval*” of the Internet since there is no need to force users and providers to adapt “*immediately*” to the new rules or software and then it results easier to be accepted. For this reason, we have imagined Trust Ecosystem as a parallel system where users are free to choose between the “*jungle*” and the trust area.

The achievement of a trust area is obviously a very complex undertaking because of the many problems to solve. While for some of the aforementioned aspects there is a broad convergence on the various proposed solutions, regarding the issues related to trust and reputation, unfortunately, effective and shared solutions are still far from being defined. For this reason, in this thesis we analyze trust and reputation in all of their aspects and lay the basis of models for the reputation management that can be effectively used in online systems and therefore included in the Trust Ecosystem.

In doing so, we have identified the theoretical aspects underlying trust and reputation and the main features that, in our view, a Trust and Reputation model must necessarily include. In this sense, we have formulated a Meta Model, called **Trust, Reputation and Recommendation (TRR-MM)** to be used as a guide for the definition of effective Trust, Reputation and Recommendation models. In addition, following the meta model, we have defined a pre-standardized e-commerce Trust,

---

Reputation and Recommendation model supporting users to make relatively better trust-based choices when buying and/or selling goods online.

## 1.2 Outline

The remainder of this thesis is organized as follows:

- the next Chapter shows the context of our research and summarizes the state of the art describing some works related to ours;
- in Chapter 3 we introduce the Trust Ecosystem and discuss some practical issues related to the implementation of the model<sup>1</sup>;
- in Chapter 4 we present the Trust, Reputation and Recommendation Meta Model and then, following it, we introduce a pre-standardized Trust, Reputation and Recommendation model for e-commerce<sup>2</sup>;
- in Chapter 5 we show several scenarios that illustrate, highlight and make fully understand advantages and potentiality of the Trust Ecosystem;
- Lastly, in Section 6 we draw some conclusions and outline future work.

---

<sup>1</sup>The content of Chapter 3 is mostly taken from the following peer-reviewed paper: [34]

<sup>2</sup>The content of Chapter 4 is mostly taken from the following peer-reviewed paper: [33]

## Chapter 2

### Research Context

In this chapter we will describe the context of our research. In doing so, we will describe the state of the art by introducing some of the main works presented in the literature highlighting both the strengths and the weaknesses. Moreover, we will discuss the aspects which need in depth analysis since we believe they have not reached a sufficient level of maturation.

Our research work has ranged over many aspects and issues related to the current Internet. We set ourselves the goal of finding a solution to augment the Internet in order to provide users with the opportunity to have a trust area to interact with higher security than at present. Therefore, the preliminary study has focused on the identification of the most critical points of the Internet users' experience and on the solutions that have been proposed so far.

In the previous chapter we described the issues that, according to our point of view, appear to be the most sensitive and should be solved soon to ensure the user that s/he can use online services in order to feel more protected. We saw that one of the main sources of uncertainty is the lack of reliability on the counterparts identity that makes users very insecure and undermines his/her interactions on the Internet. Indeed, the possibility of maintaining the complete anonymity and the guarantee of not to be traced is exploited by malicious users to the detriment of the honest ones. So, instead of ensuring users, anonymity and untraceability actually turned into strong pitfalls.

We also focused on the lack of guarantees on the counterparts reliability that

creates distrust between users, while the lack of specific information about service providers (e.g., reliability, quality, punctuality, etc. i.e, their reputation) weakens considerably online services. We pinpointed how the inability to have control and ownership of information is one of the sources of further problems since the protection of privacy is almost completely nullified. On the other hand, there is no way to prevent user contents from being reused and/or modified without any authorization or to obtain the permanent deletion from the network, nor even to claim the authorship of the same.

Finally, we also recalled how, in the digital world, users are exposed to more and more frequent identity theft.

With regard to most of the problems discussed above, in literature we can find non-integrated solutions for:

- Identity Management systems (IdMs) and Single Sign-On (SSO);
- Anonymity and privacy protection;
- Trust and Reputation Management systems (TRMs).

Nevertheless, to the best of our knowledge, there are no studies in literature that have faced all the aforementioned problems in a comprehensive, systematic and integrated view.

## 2.1 State of art

**Identity Management systems and Single Sign-On.** To use online services users are forced to create a large number of accounts at several Service Providers (SPs), each of them requiring, based on the service type, authentication credentials (e.g. login/password or certificates) and other general information (e.g. sex, age, interests, address, etc.). In practice, the SPs also play the role of authentication providers and attribute providers. The proliferation of accounts reveals several problems linked to their management, since users are forced to memorize all their credentials and to manage individual attributes. These problems could be solved using a global Single Sign-On mechanism [49, 90, 91]. **Single Sign-On (SSO)**

is a mechanism that uses a single action of authentication to permit an authorized user to access to all related, but independent, online services and resources without being prompted to log in again at each of them during a particular session. That is, the service provider sends the authentication requests to the authentication provider who is able to certify the credentials of the user who is prompted to login only once. In practice, it allows a user to access all computers and systems where s/he has access permission, without the need to enter multiple passwords by reducing human errors that are a major component of systems failure [50]. In this way, the use of Single Sign-On solves many problems related to request services from different providers.

Possession of several accounts by the same user is a source of the so-called *password fatigue or password chaos* [52, 126]. Many users, to avoid remembering multiple passwords, use the same password for all of them this causes enormous security problems since each provider is then given the key to access any of their own accounts. The use of SSO simplifies the end-user experience, avoids the *password fatigue/chaos* and enhances security [52, 108]. However, SSO also presents critical aspects. One of the most important is that users can not access to all their accounts when they are not able to connect to the authentication service (Single Point of Failure) [49]. On the other hand, a malicious user who gains access to someone else's SSO may, of course, access to all the accounts connected to it [122].

Some of the solutions proposed in literature for the SSO mainly addressed to the problem of users authentication and authorization from a *provider-centric* point of view [23, 42, 49, 90]. They are basically used to implement **Identity Providers (IdPs)** defined as the systems that control user's credentials and provide authentication services [100, 116] within individual organizations or their aggregations but they have never been used globally so far.

In recent years, the research has been oriented towards solutions, known as **Identity Management systems (IdMs)**, dealing with both authentication services and management of user identities using the user-centric paradigm [36, 42]. The IdM can be defined as framework that deal with processes for management and control of identities in online systems [36, 115]. They involve the integration of emerging technologies and business processes to create identity-centric approaches



for the management of users, their attributes, authentication factors and security privileges across the systems within multiple organizations [15].

Since the **Digital Identity**, which could be defined as a representation of an entity in a specific context [77], has become of crucial importance in the online world, users are increasingly feeling the need to simplify the management of their identity data and to increase the general level of security.

In practice, nowadays, the digital identity is managed as the equivalent of our real-life identity that is like an extended identity card or passport containing almost the same information (*who we are*) with the addition of other attributes (*what we like, what our reputation is, etc.*) [42]. Therefore, safe, reliable and user-friendly IdMs are considered fundamental in establishing trust in online interactions, such as in e-commerce applications[16, 105].

Moreover, the use of IdMs that enable SSO may help to solve the new challenges related to security and privacy protection [116]. For these reasons, IdMs have become an important and crucial research field in the management of the digital identity so that there has been a considerable increase in the number of research projects and papers in literature in this topic recently [15]. Indeed, IdMs make easier the user-experience and are considered a very safe infrastructure for the management of authentication and authorization issues. In addition, they allow the complete management of users' digital identities starting from the process of creation.

At the same time, there has been the need to increase the benefits of IdMs that, although widely used (e.g. Shibboleth [11, 79], Kantara Initiative [8], Liberty Alliance [9], Kerberos [83], OpenID [13], etc), they remain confined within one or more organizations. In fact, since to identify each user in the collaborative network has become more and more urgent, the research is oriented towards solutions that would allow the collaboration between the various IdMs [19, 125]. These solutions are known as **Federated Identity Management systems** (FIdMs) where, in general, a **federation** can be defined as the set of agreements, standards and technologies that enable a group of service providers to recognize user identities from other providers in a federated trust domain [23, 41, 116]. Therefore, member organizations of the federation must establish trust relationships with respect to the identity information (i.e. *the federated identity information*) that is considered

valid. In practice, organizations collaborate each other with mechanisms for managing and gaining access to user identity information and other resources across organizational boundaries [19].

**Anonymity and privacy protection.** As mentioned above, one of the weaknesses of the Internet that worries most users is the protection of their privacy. It is difficult or impossible to provide a thorough definition of privacy because it involves different points of view [106, 124]. From a philosophical point of view, it can be seen as a fundamental human right “*to enjoy life and be let alone*” or a basic need for a private sphere protected against others [101]. Whereas from the prospective of computer science the protection of privacy is to allow access to the most sensitive personal information only to authorized persons [14, 48, 65].

According to the European Commission Directive on Data Protection, the most sensitive personal information or personal data, called **Personally Identifiable Information** (PII), can be defined as any information concerning a natural person [70, 85]. More extensively the PII can be defined as “*the information pertaining to any living person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person)*” [12].

With the advent of social networks, the protection of privacy apart from being a right has also become a safety issue because people publish information (e.g. geo-located content, home address, when they are away from home, etc.) that can be used by malicious persons [119]. Therefore, protecting privacy can prevent personal information from being used improperly causing the lost of autonomy and freedom.

To increase the protection of privacy, some authors encourage the use of pseudonyms because they make more difficult to identify users. In fact, since the communication between two entities can also be based on their identifiers, preferably pseudonyms, it is not necessary to reveal their identity [65]. In practice, in order to maintain privacy, it should always be possible for users to be anonymous, to use pseudonyms, to choose IdPs that do not link all user transactions at all SPs together. Unfortunately, at the moment, many IdMs only implement some of these solutions based mainly on the traditional security systems [116]. In general they are based on the access control and their main aim is to provide protection from

malicious third parties.

**Trust and Reputation Management systems.** As mentioned earlier, the traditional security systems give the authenticated user a sufficient “trust” that remains constant in time. They are part of the “*hard security*” which is the first security level. These mechanisms appear to be “*safe*” for service providers who can decide on the users membership policy. However, users do not have similar mechanisms to allow them to select online service providers according to the reliability and quality of their services.

Lately, it has become of paramount importance to obtain information about trust and reputation of online service providers as well as of other users. For this purpose are used social control mechanisms including the Trust and Reputation Systems that are part of the “*soft security*” and they contribute to what is called the second-level security [93].

It is widely accepted that trust is a fundamental component of social relationships [104]. Therefore, there is the need for a support to make relatively better *trust-based choices* in the context of online interactions (e.g. *e-commerce*). Obviously, as we are in an area where subjectivity plays a predominant role, the optimal point actually does not exist and the best choice is not easy to spot.

Because of its importance, trust has been studied by many researchers in many fields (philosophy, psychology, economics, sociology, computer science, etc.). Since each discipline has defined and considered the concept of trust by its own and different perspective these definitions can not be directly applicable in the “*online world*”.

In computer science, a more accredited definition was borrowed from Psychology and Sociology [75] and sees the trust as “*a subjective expectation an entity has about another’s future behavior*” [80]. In fact in Psychology trust is a psychological state of the individual and consist in positive expectations that s/he has on the *trustee’s* intentions or behavior, that is who receives trust [96, 97, 117].

In sociology, trust is defined as “*a bet about the future contingent actions of the trustee*” [40, 112]. The bet, or expectation, is considered “*trust-based*” only if it has implications on who puts trust, called *trustor* [31, 68, 78].

So far, however, there is not an accepted definition in computer science. Other authors, define trust on the basis of its main features: *direct trust* and *recommen-*

*dation trust*. The first comes from direct experience between the parties whereas the second one is based on the experience that others have gained in their relations. In practice, the recommendation trust propagates among the members of a community. Trust increases between members if the experience is positive, otherwise it decreases. Another common definition of Trust and Distrust is that from [45]: “*Trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action*” (symmetrically for distrust). From the above, it is clear that trust is inherently personalized and assumes that there is no certainty in the prediction.

In online systems, most of the decisions are made without having any direct knowledge of the counterparts but relying only on their reputation. In these cases, the choices are typically “*trust-based*” because must be taken decisions that involve risks and do not have the possibility to verify a priori the quality of choices. A user could certainly make a better choice if he knew the counterpart reputation where reputation, according to a widely accepted definition, means “*what is generally said or believed about an entity’s character or standing*” (word of mouth) [61]. According to this definition reputation is a quantity derived from the underlying social network which is globally visible to all members of the network and it is generally based on the feedback on past interactions between members [94, 98]. In practice, the opinions that the community has expressed on the past behavior of each entity can be used to characterize and predict that entity’s future actions [37, 98].

In order to fully understand the difference between trust and reputation the following statements are usually used [61, 118]:

1. “*I trust you because of your good reputation*”.
2. “*I trust you despite your bad reputation*”.

Assuming that the two statements refer to the same interaction, we can affirm that the first indicates that the trustor is aware of the trustee’s reputation and bases her/his trust on that, while the second one indicates that the relying party has some private knowledge about the trustee, e.g. through direct experience or intimate relationship, and that these factors overrule any reputation that a person might

have. This statement shows the subjective and personal aspect of trust and that direct experiences are the most important ones. However, in their absence, we rely on the experience of the other members of the community, as expressed in the first statement.

For this purpose, the Reputation systems, which facilitate the collection, aggregation and distribution of data about an entity, are used. They are considered the only possible solution to assess the trustworthiness of users and reliability of information in online communities. Therefore, they have also become a fundamental component of the trust and security architecture of any online service [118]. Indeed they play a crucial role in the process of trust establishment and management and their importance is intended to grow up with increasing of online interactions between people and services.

In addition, Reputation systems will generally encourage good behavior over the longer term. For example, it has been shown that a good reputation improves the quality of relationships and increases the sales of e-markets [54, 95]. Unfortunately, although the use of reputation systems is widespread they are still in their infancy and are generally limited in scope. Moreover, most of the Reputation systems used in electronic markets (e.g., those used by eBay [5] and Amazon [1]) and online systems are not considered reliable because of the informal way used to assess reputation values [54, 98]. Indeed cases of “*false, misleading and inauthentic*” reviews in reputation systems as well as legal actions brought against unidentified people that provide fake reviews (e.g. [51, 113]) are becoming increasingly frequent. But the goal of a Trust and Reputation system is precisely to ensure that trust and reputation values are correct and that they were not falsified by malicious users.

As a matter of fact, a Trust and Reputation system is not effective and helpful if entities can falsely make their own reputation better or degrade the reputations of others [129]. However, over the years have been documented several types of malicious attacks focused on falsifying online trust and reputation [43, 56, 109, 110, 129]. Unfortunately, contrary to what would be desirable most of the existing approaches pay little attention to the analysis of security threats for the Trust and Reputation systems forgetting that the risks are always present [33, 43, 56, 66, 109, 110].

---

In order to be used properly, the Reputation systems should be able to deal with the trust challenges and needs of the application domain in which they are deployed. For this reason, a good Reputation system should, first of all, identify the trust needs specific to the application domain [118]. For example, a particularly important aspect to consider is that online interactions are almost never preceded by reports in the world “*offline*” [54]. Moreover, it should not be overlooked that reputational elements are intrinsically present in all online interactions such as post-counts in forums (e.g. Stackoverflow [10]), competencies in crowdsourcing (Crowdsourcing [38, 57]) and social linkages and endorsements in social networks (e.g. Facebook [6], Google+ [7]) and the social cloud [26, 27] or in modern paradigms such as Friend-to-Friend (F2F) sharing (e.g. Dropbox [4]). Another major limitation of the current trust and reputation systems is that they are confined within a specific service providers. In addition, each system collects different data types emphasizing different features. This might preclude the sharing of information between the existing trust and reputation systems. For example, it is not possible to share the information collected by Amazon with those collected by eBay because the data in their possession are not homogeneous and users cannot transfer their reputation from one system to another. Therefore, there would be the need of a global Trust and Reputation System that is independent from the individual service providers, and that is used by all the systems so that the collected information is homogeneous.

# Chapter 3

## Trust Ecosystem

The Trust Ecosystem (TEco) can be accessed by users (individuals and legal persons) and online services. All of them are considered as “*entities*” which interact with each other “*at par*” with no distinction between client and server, user and provider, services and humans. Following a user-centric paradigm, the TEco was built by integrating different innovative systems to provide the following features:

- **Trusted Digital Identity:** every digital identity corresponds to an individual (or organization) who is identified with “certainty” still keeping anonymity and privacy;
- **Content Management:** users are the owners of the information they produce and can manage such information autonomously;
- **Reputation Management:** it is possible to obtain reliable and updated reputation information about all users;
- **Interaction Agreement:** interactions are always based on a contract agreed between the parties, that have equal bargaining power.

The coexistence of these features makes the TEco a trust area. In fact, users can mutually trust as they are all identifiable, their reputation is known and while interacting, they can bargain conditions with law effectiveness. Furthermore, depending on their needs and the demands of others, users can decide which information to disseminate, protecting their privacy or maintaining complete anonymity.

## 3.1 Related Work

As previously described, we can find non-integrated solutions for: Identity Management systems (IdMs) and Single Sign-On (SSO); Trust and Reputation Management systems (TRMs); anonymity and privacy protection. Nevertheless, to the best of our knowledge, there are no studies in the literature that have faced all the aforementioned problems in a comprehensive and systematic view.

In their survey on IdMs [116], Torres et al. point out that the use of IdMs, which also enable SSO, may help to solve the new challenges related to security and privacy protection. Conversely, authors in [39, 114], highlight some of their weaknesses, especially the impossibility for a user to decide which personal information to share with every service provider or to obtain information on their reliability. To address these issues, the authors propose techniques to integrate IdMs with Reputation Management Systems, which provide information on the past behavior of the service providers [54].

Other studies, driven by the emerging of new technologies, are focused on the next generation Internet, termed **Future Internet** [84, 86, 102]. Nevertheless, they do not provide a common view on what the Future Internet is and mostly consider its network infrastructure, termed **Future Network** [116].

Despite the importance of many of the problems faced, such as infrastructural ones, we believe that even other aspects deserve attention, such as the relationship between digital identities and reputation and other little investigated sectors: the respect of user rights and the possibility for users to keep control of their data.

It is worth noting that Microsoft introduced a *Trust Ecosystem*, more narrowly defined as an environment that engenders trust and accountability between people and businesses [46]. In that system, users have several *Windows CardSpace* to access a service provider without having to authenticate [60]. Despite the similar name, our model includes more features and differs substantially from the one introduced by Microsoft, as we will show in the following.



## 3.2 Trusted Digital Identity

In the current Internet, each entity has a **Digital Identity**, which, following the definition we derived from [18], is the digital representation of the information known about a specific individual or organization. In the TEco, in addition, each digital identity corresponds to an entity in the offline world whose identity is verified with certainty. For this verification, an entity is required to register at the TEco providing access credentials, email, city of residence and its own unique identifier. For individuals, this can be the identifier used by the governments for tracking their citizens as the National Identification Number. For corporate bodies (companies, organizations, associations, etc.) it can be their VAT number. Therefore, to complete the registration to the TEco it is necessary that an entity proves to be the owner of the provided identifier. For instance, individuals could complete the registration at the Municipal Registry Office and legal persons at the Registry of Companies.

Once the registration is completed, the entity will possess a **Trusted digital Identity (TId)** in the TEco. The TId will correspond to an account associated with the identifier of the requester and it will include all the information available of him/her. The requester is the only owner of the access credentials for that account. As the TEco is only accessible to certified digital identities, online services must have a TId too. In this case, the owner of the domain name must certify the association between provider's TId and URL of the service (used as its unique identifier). The whole registration process is handled by the **Identity Management Systems (IdMs)** which assign and manage identities and belong to a **Federated Identity Management (FIdM)** [59, 71]. In general, a Federation can be defined as the set of agreements, policies, standards and technologies to achieve its objective [18, 23]. The purpose of FIdM, is to allow entities belonging to different IdMs to be identified from all others, regardless the used authentication system (e.g. Kan-tara Initiative [8], Liberty Alliance [9], Shibboleth [11, 79], Kerberos [83], etc.).

The IDMs are the only ones to know the connection between offline world entities and their TId. For this reason, an entity must own an **Internet Alter Ego (IAE)** to interact in the TEco, that is an alternative identity to present itself to others. To each IAE is associated a list of attributes, which can be *certified* or *not certi-*

*fied*. Attributes are represented with a tuple  $[name, value, url\_of\_certifier]$  where: *name* represents the attribute name, which can be standard (e.g. *date\_of\_birth*) or user-defined (e.g. *preferred\_wine*); *value* is the value of the attribute which can be either a string or an *url\_of\_value* that indicates where the attribute value is located (e.g. a link to the *City* attribute in *Google+* profile). *url\_of\_certifier* refers to the entity that certifies the content of the *value* field. Obviously, if the attribute is *not certified* this field is empty.

As we already pointed out, when a user is accredited to the TEco, the IdM creates an account for user's TId that can be considered as a sort of *Meta IAE* of the user. Initially, the IdM only fills the account attributes received from the certification institution (e.g. for individuals, name, surname, address, etc.). Later, the *Meta IAE* will be filled with all the other user's attributes. Indeed, when the user creates new attributes to be added to his/her IAEs they will also be added to the *Meta IAE*. Similarly, the *Meta IAE* will also be filled with the certified attributes created by the institutions with whom the user interact (e.g. achievement of a new degree, see scenario 5.7).

Based on his/her needs, an individual can create different IAEs (e.g., as a researcher, as a chess player, etc.), choosing for each IAE which information to show among those associated to his/her own TId (i.e. *Meta IAE*).

In general, after the user has accessed the TEco s/he can use his/her IAEs without any restriction. In order to improve security, the user can set access credentials for some IAEs.

Each IAE is completely independent from the others and is seen by counterparts as a separate entity. In fact, a counterpart cannot relate all the IAEs belonging to the same identity. This safeguards an entity's privacy, since it can use one of its IAEs without worrying that its true identity is revealed or that one of its IAEs is associated to others (in the following, we will see how this can be guaranteed through the use of temporary identifiers).

Each entity must choose a *reference IdM* in the FIdM which will manage its TId. A registered entity to access the TEco must logon at the *reference IdM* through the planned identification procedure (e.g. based on username/password, biometric data, cognitive fingerprint [25, 47, 67, 123], etc.). Then, the entity receives from the IdM the list of all its own temporary identifiers, referred to as

*TempIAEs*, specifically generated. Each of them uniquely identifies a specific IAE and allows the entity to interact within the TEco without logging on to any specific service. This enables a SSO authentication. While the entity is “connected” to the TEco, the *reference IdM* periodically regenerates the *TempIAEs* and it sends them back to the entity according to predefined security criteria or upon an entity’s explicit request. It should be noted that the regeneration of the identifiers does not require a new logon. The *TempIAEs*’ validity expires as the entity “disconnects”, by logging out after an indefinite time.

Besides identity management, the TEco also provides a reputation system based on several **Reputation Management Systems (RMSs)**, each responsible to collect, aggregate and disseminate data on the reputation of the entities [54]. The RMSs belong to a **Federated Reputation Management System (FRMS)**, which manages their interaction. The integration of FRMS and FIdM provides the users with a high level of mutual trust. In fact, they are encouraged to take appropriate behavior because they know they are identified with certainty and their past behavior is known to all. The greater mutual trust increases the *social capital*, intended as the richness of the interactions between members, which itself affects the reputation system encouraging an active and honest participation and thus increasing its effectiveness [103].

The FIdM assigns each entity a *reference RMS* which is also involved in managing the reputation of all its IAEs. At the end of an interaction, an entity is required to leave an anonymous feedback on the counterparts to its reference RMS. The latter, in turn, according to the times and rules set by the federation, sends the feedback to the reference RMS of the recipient entity. An entity can request the reputation of the other entities to its own reference RMS, which obtains it through the federation. It is worth recalling that, being independent, each IAE has its own reputation independently from others. Since a good reputation requires time, this reduces the proliferation of IAEs (see “newbies” in [33]).

### 3.3 Inter Pares Interaction

In the current Internet, the users share information and request services by establishing interactions. In the TEco, any interaction is always based on a contract agreed between the parties. We refer to the interaction as **Inter Pares Interaction** (in the following referred to only as “*TEco Interaction*”) and to the contract as **Negotiated Interaction Agreement** (in the following referred to only as “*negotiated agreement*”). The negotiated agreement is composed of two parts: the first, preliminary and fixed, contains the principles and general conditions that oversee any interaction in the TEco (e.g., to respect owners’ constraints on the data, not to maliciously alter reputation, etc.). The second part is subject to negotiation and contains a list of **Agreement’s Terms** (in the following referred to only as “*term*”), i.e. constraints and preferences established in a formal language, that the parties agree to comply with. If some constraints in the *negotiated agreement* are not respected by one of the parts, as terms of a contract with the force of law, can be asserted in judicial offices. Since, as stated in [33], an entity interacts with the others in a given context and assuming a specific role, an **Interaction Context/Role (ICR)** for each entity in the *negotiated agreement* will also be mandatorily negotiated. For instance, the consultation of a website is a typical “interaction” between end-user and website owner, where the ICRs are: “*Website/Surfer*” for the end-user and “*Website/Owner*” for the website owner.

The *negotiated agreement* is established through a phase of **Negotiation of the Agreement** (in the following referred to only as “*negotiation*”), in which each party sends the other its contract proposal, called **Interaction Agreement** (in the following referred to only as “*agreement*”), composed of the list of *terms* that a party intends to include in the second part. During negotiation, each *term* can be modified or accepted to reach the *negotiated agreement* in its final form. If all parties agree, the *negotiated agreement* can be changed at any time. Clearly, an entity that does not conclude the phase of *negotiation* can not take part in the interaction.

The *terms, agreements e negotiated agreements* are defined through a formal language. This allows the entity to participate to the *TEco interaction* through an **Internet Agent**, which suggests or takes decisions on the basis of its acquired

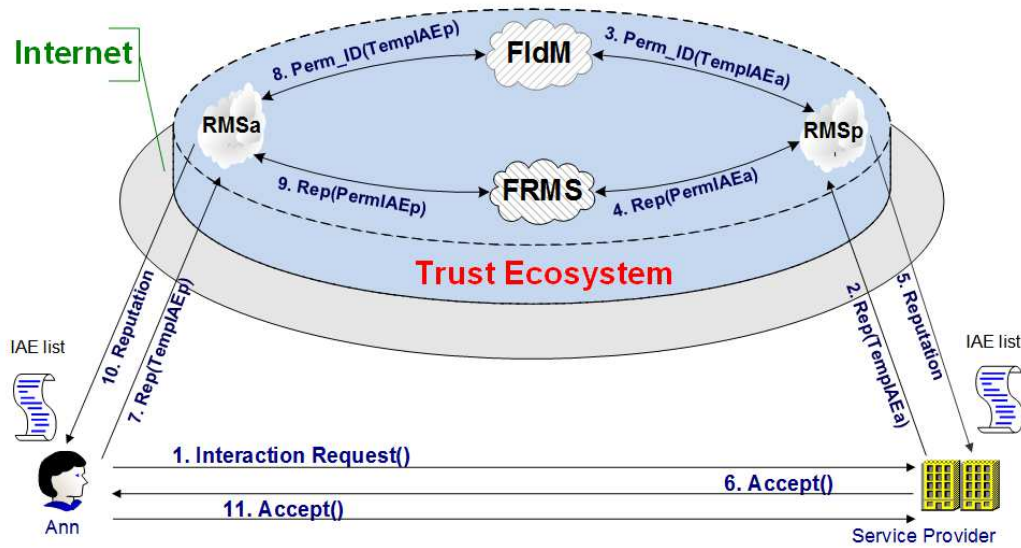


Figure 3.1: Interaction between entities in the TEco.

experience (self-learning), on the type of entity (e.g., individual) and on the context/role (e.g., e-learning/instructor). For instance, in the case of an individual, human intervention may be required during bargaining. In the context/role e-commerce/seller, the *negotiation* phase of the seller is automatically handled by the Internet Agent and the human intervention is not required, unless expressly prescribed by the seller. It should also be pointed out that an *agreement* can be defined by including only standard *terms* that are stored in an archive at the FIdM which also manages an archive of default *agreements*. A new *agreement* is created by choosing the *terms* from a list of standard ones through an appropriate GUI. In order to simplify the *negotiation* phase, while logging on to the TEco, the entities receive (similarly to IAEs) lists of predefined *terms* and *agreements* from the FIdM. This way, they can set an *agreement* for each IAE choosing it from the default ones. For instance, the entity could select an IAE called “*Web surfing*” associated to an *agreement* called “*High Privacy*”, requiring counterparts not to request private information such as the *home address*.

Figure 3.1 shows how two entities establish a *TEco interaction* (the schema can be extended to more than two entities). We use the following notation: **TempIAE** for the temporary identifier of an entity’s Internet Alter Ego; **PermIAE** for the

permanent one. It is worth recalling that permanent identifiers are never disclosed to entities. As shown in the Figure, to establish an interaction in the TEco the following steps must be executed:

- Step 1. *Ann* requests an interaction to a service provider (SP) providing IAE's temporary identifier (*TempIAEa*) with which she intends to identify herself and her *agreement*. Besides indicating her Context/Role (*ICRa*), *Ann* must also communicate to the provider the Context/Role (*ICRp*) with which the provider will have to interact.
- Step 2. The SP requests to its reference RMS (*RMSp* in the figure) the reputation associated to *TempIAEa* and related to the context/role (*ICRa*) provided by *Ann* in her *agreement*;
- Step 3. *RMSp* requests to the FIdM the permanent identifier (*PermIAEa*) associated to *TempIAEa*;
- Step 4. Once obtained the *PermIAEa*, *RMSp* checks if it has the reputation associated to *PermIAEa* in the context/role *ICRa*. If not, *RMSp* requests it to the FRMS.
- Step 5. Then, *RMSp* returns to SP the reputation of *TempIAEa* in *ICRa*. It is worth nothing that SP receives the reputation of *Ann*'s IAE knowing only her temporary identifier.
- Step 6. SP decides, based on the received reputation, whether to accept the TEco interaction request. If so, SP sends *Ann* the IAE with which it intends to interact (*TempIAEp*) and its own *agreement*. Otherwise, it sends a message of rejection and abandons the interaction.
- Steps 7-11. The same actions performed in Steps 2 - 6 on *SP*'s side are executed on *Ann*'s side. Step 11 opens the negotiation phase which ends with the negotiated agreement.

The way to establish a *TEco interaction* was schematically shown in sequential steps in order to facilitate the exposure but, actually, some steps may be performed in parallel (e.g., the negotiation phase). As previously mentioned, the parties may

express a feedback on counterparts at the end of the interaction.

Nevertheless, to prevent malicious attacks [101] and improve the reputation system, the TEco adopts some important countermeasures already described in [33]. After the negotiated agreement is established and before starting a *TEco interaction*, an entity's Internet Agent sends its *reference RMS* a list of pairs (IAE; ICR), each referred to an entity it is going to interact with. The RMS, in turn, sends back the **Interaction Token** with which the interaction will be uniquely identified for a predetermined time interval. This token allows the RMS to accept only feedbacks to and from entities that indeed took part to the interaction and to make sure that the interaction indeed took place. Therefore, every feedback must include the *interaction token* and the *TempIAEs* of both the judging and the judged entities. This assures that a feedback is expressed once for each entity involved in an interaction.

Furthermore, the RMS could release encrypted reputation data with date and time of encryption. This ensures data integrity and authenticity. This also speeds up the reputation retrieval, since entities may store the encrypted reputation data and share them with counterparts without querying the FRMS. Counterparts may decide whether to query the FRMS on the basis of both the certification date and the reputation of the entity (too old data may be untrustworthy). We remark that the presence of a contract having the force of law strongly discourages illicit practices, as they can be prosecuted.

### 3.4 Content Management Framework

As mentioned before, one of the objectives of the TEco is to ensure that the entities are direct owners of the information they produce. To this aim, an important role is played by the **Content Management Framework (CMF)**, which manages all data (text, multimedia, IAE's attributes, etc.) related to the entities. Whenever a new content is created at a service provider, the CMF automatically creates a link between the content and the producing entity. These data are physically stored at the SP or in personal cloud storage systems, local hard disks, etc. In any case, they

are property of the entity that produced them, which can decide which *access rights* to grant to other entities (reading, modification, deletion, duplication, disclosure, etc.). Furthermore, the time validity of each *privilege* can also be established. Therefore, contrary to what normally happens in the current Internet where the users are deprived of these rights, in the TEco the users have management and responsibility of their own data. The CMF ensures that the rights set by the content owner, with any changes, are disclosed to the other entities and that they respect such rights. To this end, the CMF tracks the use of contents by entities and, in case of infringement of privileges, it requests the FRMs to lower the reputation of the infringing entity and, in extreme cases, that it is excluded from the TEco. Another duty of the CMF is to “certify” with legal value the publication of a content on the Internet. This feature is strongly felt by many users in the current Internet. Let us consider, for example, the case of a university that has issued a call for a research grant. The CMF must certify: 1) that the URL of the content is accessible at any time (**Where**); 2) the date and time (timestamp) of the publication (**When**); 3) the integrity of the content (**What**); 4) the authenticity of the publication, i.e., that it comes directly and truly by the entity (**Who**). If the content is modified after publication, the CMF certifies the four *W* for all the previous versions, which are still stored (*versioning*) and made public. As for RMSs, the CMFs are also part of a federation, called **Federated Content Management Framework (FCMFs)**, which manages their interaction.

### 3.5 Discussion

The TEco is an incremental model which enhances the current Internet without replacing it. This is one of its strengths as it requires no upheavals in infrastructures. Furthermore, it does not compel users to adapt to new rules or new software. The TEco can be developed in parallel with the Internet, leaving the users free to choose between a deregulated area and a trust area, exactly as in the offline world. To make it applicable it is necessary that the systems described so far, federated Identity Management system (IdM), federated Reputation Management System (RMS) and federated Content Management Framework (CMF) are implemented



and integrated bearing in mind the characteristics described in this section.

To obtain the permanent identifier associated to a *TempIAE* (see Figure 3.1 - Steps 3 and 8) from the federated IdM, the federated RMS must use a specific communication protocol that may be similar to the protocols used in Internet to resolve domain names. This protocol must ensure that the association between permanent and temporary identifiers is known only to the two federations. The implementation of federated RMS also requires that an ontology of the Contexts/Roles and, for each of them, the Main Features are identified, as explained in [33], to which the reader should refer for further details.

It is necessary to define a formal language for the specification of Agreement Terms and Interaction Agreements and to define Standard Agreement Terms and some predefined Interaction Agreements. It is also crucial for the success of the TEco the implementation of an efficient Internet Agent that facilitates entities in all activities related to the TEco. In particular, it could include a plugin which works during Web navigation (e.g., as done in [32]). This plugin would allow an entity to request a *TEco Interaction* by simply entering the address of the website in the browser and specifying the alter ego s/he intends to use. It will then be the Internet Agent to handle the request by interacting with the service providers (see Figure 3.1 - Steps 1 and 6). A *TEco Interaction* will be established if and only if the service provider, which also owns a Trusted Digital Identity (TId), accepts the request. In both cases, the navigation would continue normally, except that a *TEco Interaction* will enable all the benefits of the TEco (negotiated agreement, SSO, reputation, etc.) and a browser icon will indicate that the transaction is performed in the trust area (as in https). A protocol for negotiation of the agreement is also necessary to allow the Internet Agents to perform it autonomously.

As already mentioned, the federated CMF has to manage all the contents and information related to a TId. It uses the same procedure described previously for the management of the attributes of IAE, i.e., each content is represented with a tuple *[name, value, url\_of\_certifier]*. Furthermore, since each attribute of the TId can be considered as a content, it will also be managed by CMF. Whenever a new attribute of an entity is declared, a new record will be added in the CMF. For instance, following the achievement of the PhD in computer science, a new record like *[PhD, PhD in Computer Science, www.unisa.it/PascuccioFA/CSPHD]* will be

added for the corresponding TId. To simplify the handling of content for an entity, its Internet Agent could support the user during the creation of new contents. For instance, when a user publishes in a blog, his/her Internet Agent suggests a default repository (the user can chose another one) in which to store the data and then sends a link to the content to the blog. If the content is already present in the CMF, the user can simply choose the link without rewriting the text. This would be totally transparent to the user, who would only compose the content through an appropriate GUI, while all other activities would be carried out independently by the Internet Agent.

## Chapter 4

# Trust, Reputation and Recommendation Meta Model

In recent years there have been numerous studies aimed at understanding how to manage online trust and reputation. Nevertheless, in our opinion, all of these studies have not gone in the same direction. In fact, according to [44, 55, 73, 120, 121], we recognize the lack of shared bases and goals. Authors in [64] also recognize the lack of a unified research direction and note that there are no unified objectives for trust technologies and no unified performance metrics and benchmarks.

In fact, there are many models in the literature that treat trust and/or reputation contradictorily. For instance, some models use calculation methods based on the transitivity of trust while some authors demonstrate that trust is not transitive but propagative [103]. Other models calculate trust/reputation without taking into account properties deemed essential by some authors (e.g., context-specific, event-sensitive, etc.) [61, 103].

Lastly, differently from other areas of computer science, there is not a well-defined set of testbeds for comparing models [44]. Validations are not performed through a comparison of the results with other models because often they are neither reproducible nor comparable [63]. Almost always the data are not shared and therefore validations use different data even in the same application domain [69]. It rises from the above reasons the urgency of reaching a standard trust and reputation model.

In this Chapter we lay the foundation for the formulation of a meta model to be shared with researchers in the field, defining properties, characteristics, methods and best practices to which Trust, Reputation and Recommendation (TRR) models should be compliant. We draw inspiration from similar proposals in the literature [64, 73, 74, 120]. Our meta model is also the result of a critical review in which we have recognized strengths and weaknesses of the most important existing TRR models [17, 61, 99].

However, differently from the above cited works, we define a meta model with real requirements for the definition of TRR models. The main purpose of the meta model is to facilitate the definition of a generic TRR model. In fact, the meta model explains how to create, step-by-step, a compliant model. Among others, a standardization is needed to determine the fundamental properties which must be present in a TRR model, thus avoiding that the models do not take them into account. Designing a TRR model in a standard manner will also facilitate the reuse of some of its parts.

Another goal is to introduce a pre-standardized TRR model for e-commerce. Obviously our model does not claim to be final, since the intention is to propose a basis on which researchers will be able to discuss and, “speaking the same language”, establish a common objective and select the best proposals [61].

In the following we firstly describe related work; then we present our meta model. Finally, we introduce a pre-standardized TRR model for e-commerce following our meta model and then we draw some conclusions and outline future work.

## 4.1 Related Work

Several papers [61, 87, 103] review the most important TRR models. Conversely, to the best of our knowledge, only a few propose meta models to facilitate the definition of standard models. Many authors, among which [44, 64, 73, 120, 121, 128], emphasize the lack of common understanding and shared description in trust models.

Authors in [73] describe an interesting pre-standardized approach for trust and/

or reputation models for distributed and heterogeneous systems. They also survey several representative trust and reputation models, describing their main characteristics, with the objective of extracting some common features from them in order to obtain a set of recommendations for a pre-standardized process. In their view, a generic model should consist of the following five components: *gathering behavioral information; scoring and ranking entities; entity selection; transaction; rewarding and punishing entities.*

Authors in [128] deal with the *federated trust management*. Trust management in federated environments, as in service-oriented architecture (SOA), will introduce additional complexity. In these environments, it is necessary that different trust management systems can interoperate. Complexity increases because, as many authors complain, there is no consensus on what constitutes the trust. There is the need for a way of representing trust that may be understood by all parties involved. Authors also stress the need for a shared understanding and they identify important aspects of trust frameworks. In order to systematically study the requirements rising from federated trust management, they classify these problems into five aspects: *trust representation; trust exchange; trust establishment; trust enforcement; trust storage*. Then they propose a conceptual architecture for federated trust management.

An approach for building a generic trust model, called *UniTEC*, is also described in [64]. Authors identify the following dimensions of the trust relationship: *trust measure; trust certainty; trust context; trust directness; trust dynamics*. Then, they map these concepts on the components of their generic trust model. With this approach, built on the observation, the outcome of each trust model can be mapped onto *UniTEC* and it is also possible to compare models with each other. However, during mapping to the generic trust model details of the trust model are lost [120].

Authors in [120] created a generally applicable meta model, called *TrustFraMM*, which aims at creating the common ground for future trust research in computer science. As authors declare, their meta model was born from the idea of identifying identical functionalities in different available trust frameworks. Using their meta model any trust framework can be described as a set of standard elements of the *TrustFraMM*. The authors expect to get several common implementations so that it will be possible to apply Model Driven Architecture to trust

management. This way, it will be easier for researchers and developers to find new solutions also in domains that have not yet been explored. The proposed meta model is only at its first version. The authors plan to further detail the identified elements taking into account the proposals of the other researchers.

In [121] the *TrustFraMM* meta model is extended to be used in the design process. The authors describe a systematic approach for the design of trust frameworks. The basic idea is that in trust framework design there are typical aspects that restrict the possible solutions. For this reason, the authors believe that, by using tested and approved procedures, the design of a trust framework is an exploratory process. Therefore, a designer can select the elements of *TrustFraMM* suitable for his/her specific implementation.

An investigation of trust-based protocols in mobile ad-hoc networks is reported in [92]. The authors also provide a set of properties and essential concepts that should necessarily be considered by trust framework designers in these environments. In addition, methods for the management of trust evidences are categorized. Although some concepts are only briefly exposed and not explained in detail [120], the work provides some important insights on trust management.

As remarked in [110] and [111], the existing works do not well address how to request and obtain recommendations and how to manage attacks and protection mechanisms. Our meta model, besides identifying some crucial aspects in the building of trust/reputation, addresses researchers on how to “*think of*” and define a standard TRR model. The meta model “forces” to deal with some fundamental aspects which are often neglected in many of the proposed TRR models.

Lastly, our TRR model for e-commerce provides both an application of the proposed meta model and many starting points about trust and reputation management.

## 4.2 Definition of the TRR-Meta Model

In this section, based on observations and literature, we define a TRR meta model whose objective is to facilitate the definition of TRR models and the identification of standard models for any particular context.

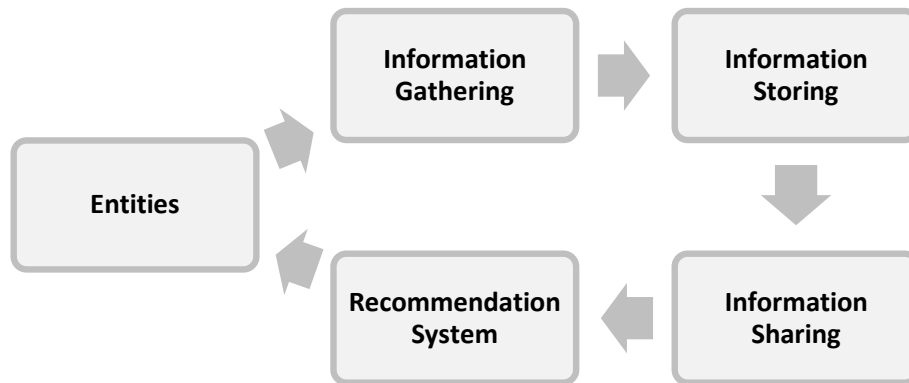


Figure 4.1: TRR Meta Model - Main Components of Information Management.

Our meta model has been divided into two parts, which list a series of information that shall be provided to build a TRR model compliant with our TRR meta model. This information will also be useful to make the various TRR models more understandable and classifiable. Part 1 is preliminary for the second and covers the fundamental principles and the basic information on which the TRR model is based. Part 2, instead, specifies the way in which information is handled, i.e. it contains the actual definition of the model.

Following our meta model every TRR model should provide a mechanism to gather the information produced by the entities participating in the system. Then this information should be stored and made available to a recommendation system. This one, using this information, will advise the entity with which counterpart to relate to, according to its needs. Figure 4.1 shows the components of our TRR meta model for the information management.

As mentioned in Section 1, in this section we will only list the requirements of the meta model, and will motivate and explain in more detail the choices made in the next section, where we will apply the meta model to define our TRR model for e-commerce.

### 4.2.1 TRR Meta Model Part 1 - Basic principles

1. *Scope*. The community referred to by the TRR model (e.g.: social networks, company, e-commerce, etc.). This information is useful to classify the model;
2. *Goals*. The objectives of the TRR model. This information is necessary to let researchers and developers properly use the model.
3. *Fundamental Concepts*. Basic concepts underlying the TRR model justifying the choices made. This point should be carefully described, as it is very important to have solid and commonly accepted basic principles on trust and reputation otherwise the proposed solutions lack any foundation.
4. *Contexts/Roles Ontology*. All the contexts/roles in which the TRR model can be used (e.g. *e-commerce/buyer*, *e-commerce/seller*) [17, 64, 120]. Although it may be challenging to identify the most suitable contexts/roles ontology, it is still essential to have a shared basis on which to think and discuss. Without a shared ontology of contexts it will be complex to reuse metrics or parts of models defined by other authors. Therefore, following the fundamental concepts at the previous point, the TRR model shall specify:
  - (a) *Context/Role Main Features (MF)*. The main features that contribute to build the trust (reputation) for each context/role (e.g. “*quality*”, “*reliability*”) [61, 103].
  - (b) *Main Features Values (MFV)*. Value domain which can be assigned to each MF (e.g. “*good*”, “*poor*”, [0,1], etc.).
  - (c) *Main Features Measurement*. The metrics for each MF. They shall respect two conditions:
    - i. Negative ratings decrease the value of the MF;
    - ii. Positive ratings increase the value of the MF;
  - (d) *Trust/Reputation Measurement*. The specific metric for trust/reputation for each context/role (it is possible that some contexts/roles share the same metric);



5. *Malicious Attacks.* List of all attacks that can undermine the TRR model [56, 110]. A detailed understanding of the threats that may make the model unreliable helps to define a more effective TRR model. Many models are defined without taking into account the malicious attacks. This point shall be constantly updated as new attacks are periodically identified;

#### 4.2.2 TRR Meta Model Part 2 - Information Management

1. *Entity management.* The entities shall be distinguishable from each other within the system, otherwise it would be impossible to assign a value to their trust/reputation. For this reason it is necessary that the TRR model defines how the involved entities are managed. In the management of the entities (users, services providers, etc.) the following aspects shall be kept in mind:
  - (a) *Longevity.* After each interaction with an entity there should be the possibility of having other interactions with it in the future [61]. In practice, it shall be impossible or difficult and above all not convenient to change identifier.
  - (b) *Privacy.* The protection of privacy has become a crucial aspect and more and more users require that their private data are protected. An unclear privacy policy may discourage the participation of honest users. It should be specified whether and how the privacy of users is protected;
  - (c) *Anonymity.* It should be specified whether and how the users have the option to be anonymous;
  - (d) *Initial values.* It shall be specified which initial values are assigned to the trust/reputation of the new entities (newcomers). The assignment of an incorrect or not consistent initial value to newcomers could affect the effectiveness of the system. This is almost always ignored in many models;
2. *Information Gathering.* It shall be specified in which way the values of the main features are gathered for each context/role [73, 82, 120]. Therefore, the TRR model shall specify:

- (a) which *passive* mechanisms (without user intervention) for information gathering are used;
- (b) which *active* mechanisms (the user gives explicit feedback) for information gathering are used;
- (c) how the authenticity of the information is preserved (*Authenticity*).

In any case, the values collected or assigned by the user must be consistent with those reported in Part 1.

3. *Information Storing*. Besides indicating how the information on the MFs is stored, the TRR model shall specify:
  - (a) whether one party of a transaction (agent/resource) cannot deny having received/expressed a rating (*Non-Repudiation*);
  - (b) whether and how the information is aggregated (*Aggregation*);
  - (c) whether and how the oldest information is taken into account (*History*);
  - (d) whether and how the oldest information is less influential than the most recent (*Aging*);
4. *Information Sharing*. All users shall have access to the same information (*Democracy*). The TRR model may specify:
  - (a) whether all the necessary knowledge (rules, procedures, etc.) to interpret and manage the information shared by the system is made available (*Knowledge*);
  - (b) whether the information is easily understood (*Clarity*);
  - (c) whether the system is easy to use (*Usability*);
  - (d) whether it is possible to trace or contact the raters (*Untraceability*);
5. *Recommendation System*. A mechanism to “advise” the user which entities to interact with in a given situation (context/role). Some systems may only collect and share information about the entities. If the TRR model includes a recommendation system, it shall describe in detail the “decision-making process” used;

6. *Incentive Mechanism*. After a transaction, the users usually have no incentive to give a rating about the other party. To be successful, a TRR model should encourage the participation of honest users and discourage dishonest behavior [61]. Therefore, being this a fundamental aspect, the TRR model should describe in detail the *incentive mechanism* used [62];
7. *Malicious Attacks Resilience*. In general there can not be a system completely immune from attacks by malicious users. Nevertheless, it is possible to make malicious behaviors inconvenient. The TRR model should indicate whether the system is resilient to the attacks listed in the first phase and if there are weaknesses.

### 4.3 A Pre-Standardized Trust and Reputation Model for E-Commerce

In this section, we propose a pre-standardized TRR model for e-commerce whose definition has been carried out following our TRR meta model. Here we outline the features that, in our view, must necessarily be part of a standard model. The purpose of this section is to provide an example of application of our meta model, which is helpful for creating models for various contexts (e.g. *product review; expert sites; autonomous system; wireless sensor networks; mobile ad-hoc networks; mobile agent system; service-oriented architecture; etc.*).

#### 4.3.1 TRR Model for E-Commerce Part 1 - Basic principles

1. *Scope*. The model is applicable in the context of selling products online (e-commerce).
2. *Goals*. Providing an entity with reliable information on the conduct of the other party in the context/role in which they will interact.
3. *Fundamental Concepts*. A common definition of Trust and Distrust is that from [45]: “*Trust is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform*

*a particular action*” (symmetrically for distrust). We adopt the definition of *trust* based on the former encounters between two agents: “*Trust is a subjective expectation an agent has about another’s future behavior based on the history of their encounters*” [81]. Here an “*encounter is an event between two agents within a specific context*”.

Furthermore, we adopt the following definition of Reputation: “*what is generally said or believed about an entity’s character or standing*” (*word of mouth*) [61].

Reputation clearly has a global aspect whereas trust is viewed from a local and subjective angle.

In the light of the above arguments, a recommendation system, besides relying on reputation, should allow an entity to consider any private information in its possession (direct trust). For example, an entity may build its own *trust-chain*, i.e. a periodically updated local store which includes trust data of the other entities of which the entity has direct knowledge.

As regards trust and reputation, in agreement with [61, 88, 103], we consider of primary importance one aspect that is often overlooked by many authors: *Trusting Ann as a doctor is not the same as trusting her as an aircraft pilot*. This is also true for the reputation and suggests that trust and reputation are dependent on the context and the role (*Context/Role-Sensitive*). Therefore there can be no single evaluation method for trust and/or reputation that is applicable in all contexts/roles and thus it is essential to identify a *Contexts/Roles Ontology*.

In addition, each context/role has its own peculiar characteristics (main features) that contribute to a greater extent to build trust (*subjective expectation*) or reputation (*word-of-mouth*) of an entity. For instance, a high level of trust (reputation) in an online store might arise from its positive ratings received on *product quality, assortment*, etc.

Another major point is the way in which inhomogeneous values are commonly aggregated. In fact, the aggregation of all the features values in a single trust (reputation) score causes a significant loss of information, and produces an unreliable result. For example, we believe that aggregating the

ratings regarding *product quality* with those regarding *assortment* has neither a logic nor a theoretical justification. For this reason, in our model we maintain separate values for each main feature.

In this section we cannot ignore a series of other fundamental properties of trust and/or reputation [61, 103]:

- (a) *Subjective*: subjective nature of ratings leads to personalization of trust/reputation evaluation.
  - (b) *Relational*: as two members interact with each other frequently, their relationship strengthens, and trust (reputation) will increase if the experience is positive and decrease otherwise.
  - (c) *Dynamic*: trust and reputation decay with time, hence new experiences are more important than old ones.
  - (d) *Propagative*: if Ann knows Bob who knows Clair, and Ann does not know Clair, then Ann can derive some amount of trust on Clair based on how much she trusts Bob and how much Bob trusts Clair.
  - (e) *Non-Transitive*: if Ann trusts Bob and Bob trusts Clair, this does not imply that Ann trusts Clair. Propagation does not imply transitivity.
  - (f) *Asymmetric*: Ann trusts Bob does not imply that Bob trusts Ann.
  - (g) *Slow*: high trust and good reputation take a long time to build, i.e., they grow slowly.
  - (h) *Event sensitive*: a single high-impact event may destroy trust (reputation) completely.
  - (i) *Indirect Trust*: trust can be based on second-hand information about an entity that one does not know directly.
  - (j) *Direct Trust*: first-hand information should always be the most reliable.
4. *Contexts/Roles Ontology*. In the context of e-commerce we identify the following contexts/roles: *e-commerce\seller* and *e-commerce\buyer*.
- (a) *Context/Role Main Features (MF)*. We identified the following main features (see Figure4.2):

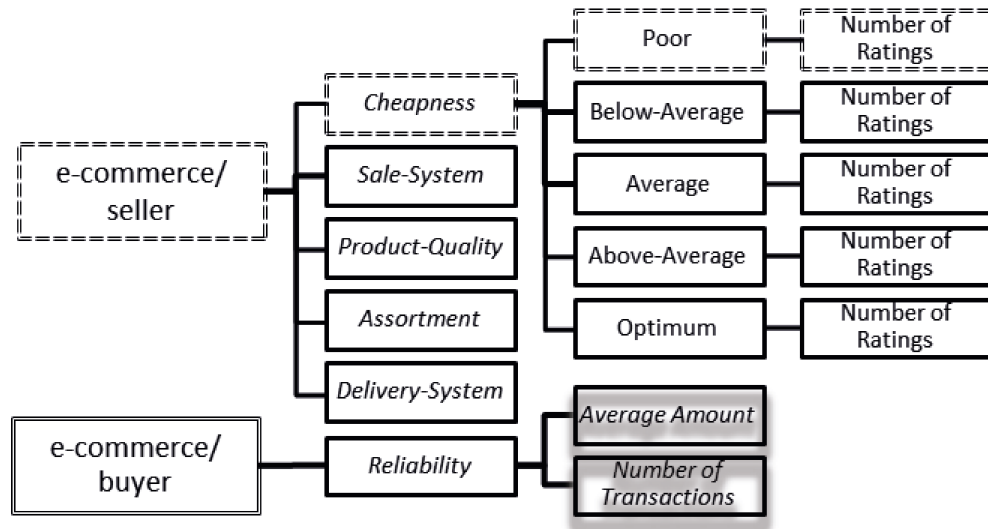


Figure 4.2: Categorization of the information according to: context/role, main feature and main feature values.

- e-commerce/seller: *Cheapness, Assortment, Delivery System, Sale System and Product Quality*;
- e-commerce/buyer: *Reliability*;

(b) *Main Features Values (MFV)*. The following values can be assigned to all main features in the e-commerce\seller context: *poor (P)*, *below average (BA)*, *average (A)*, *above average (AA)* and *optimum (O)*. The amount of the transaction (values in **R**) is assigned to the *Reliability* main feature in the e-commerce\buyer context.

(c) *Main Features Measurement*. For each MFV in e-commerce/seller, the Number of Ratings (NoR) received is stored. Since each rating will increase the NoR of the MFV, the following properties are valid:

- i. Every negative rating decreases the value of the feature. In fact, it increases the NoR associated with the corresponding negative value;
- ii. Every positive rating increases the value of the feature. In fact, it increases the NoR associated with the corresponding positive value.

For each MFV in the e-commerce/buyer, two values are kept: number of transactions (necessary to recalculate the average) and the average amount spent (the actual measure of the Reliability). The following properties are valid:

- i. Transactions with a spent amount lower than average decrease the value of the feature;
  - ii. Transactions with a spent amount higher than average increase the value of the feature;
- (d) *Trust/Reputation Measurement*. As shown in the following, the model does not deal with the computation of a value for trust/reputation. It only collects information on the past behavior of the entities, that is made available for subjective evaluations.
5. *Malicious Attacks*. The most common attacks are the following (detailed definitions are in [43, 56, 110]):
- (a) *Whitewash*: a user with a poor reputation, obtains a new identity to erase his/her previous reputation;
  - (b) *Sybil Attacks*: a dishonest user attempts to obtain multiple identities to cheat the reputation system;
  - (c) *Traitor*: a user with low reputation behaves well until s/he reaches a good reputation. Then s/he resumes his/her dishonest behavior;
  - (d) *Fake transaction*: a user creates ad-hoc transactions only to express a rating. Although transaction costs may be required, it could be equally convenient to bear the costs in relation to the benefits achieved;
  - (e) *Slander*: a user acquires many identities (sybil attack) and then provides negative feedback to decrease the reputation of the victims;
  - (f) *Promote*: a user acquires many identities (sybil attack) and provides positive feedback to increase the reputation of a target;
  - (g) *Slander+Promote*: both Slander and Promote are exploited at the same time;

- (h) *Self-promote*: a user gives positive feedback on subjects in whose s/he is not interested to increase his/her own reputation, and then provides dishonest feedback on the victims;
- (i) *Oscillation*: some users acquire many identities (sybil attack) which are divided into two groups with different roles. A group focuses in giving dishonest feedback on target, while the other focuses in increasing its reputation by providing honest feedbacks. The roles of the two groups dynamically alternate;
- (j) *Ballot stuffing*: a user gives many ratings so as to affect the reputation of the target;
- (k) *RepTrap*: some users acquire many identities (sybil attack) forming a coordinated group to become “majority”. The group gives many negative ratings on the targets (users with a few feedbacks, called “traps”) to exceed the majority of feedbacks. In this way, the system will judge the negative feedback expressed by dishonest users as “consistent” with the reputation of the target and, on the other hand, as “inconsistent” the feedback provided by honest users.  
The final effect will be that the honest users will have their reputation lowered and the dishonest users will have it increased. Many traps will be disseminated in the system. The side effect is also to reduce the total number of honest users with high reputation;
- (l) *Denial of Service*: a DOS is caused to avoid the calculation and dissemination of reputation;
- (m) *Exit*: a user who has decided to leave the system is no longer interested in his own reputation and can behave dishonestly without worrying about the consequences;
- (n) *Context/Role Sliding*: a user attempts to gain a good reputation in the contexts/roles where it is easier and cheaper to get it and then have malicious behaviors in other contexts/roles exploiting the high reputation gained;
- (o) *Orchestrated*: a user organizes attacks using various of the strategies



listed above;

### 4.3.2 TRR Model for E-Commerce Part 2 - Information Management

1. *Entity management*. This model works with any Identity Management. Necessary and sufficient condition is that the entities are *distinguishable* from each other.
  - (a) *Longevity*. Even though the entities can change their identifier, it is not advantageous: the newcomers are recognized because they have a few ratings.
  - (b) *Privacy*. Neither data on users nor data on content of transactions are stored, thus privacy is preserved. Furthermore, the average value of purchases it is not a “sensitive” information (see next point 3);
  - (c) *Anonymity*. The users are uniquely identified by an identifier and therefore remain anonymous;
  - (d) *Initial values*. Newcomers have no initial assigned value;
2. *Information Gathering*. Following a transaction, the buyer (seller) can express his own evaluation of the seller (buyer) (*relational property*). Users, depending on the context/role, shall express a rating on the specific MFs identified in Part 1.
  - (a) The ratings expressed by the seller against the buyer (the amount of a successful transaction) could be automated and considered a passive mechanism for information gathering;
  - (b) The ratings expressed by the buyer against the seller (explicit feedbacks) are an active mechanism for information gathering;
  - (c) Information authenticity can be preserved using SAML assertions [22];
3. *Information Storing*. As mentioned in Part 1, a rating produces a list of values, one for each MF in the context/role. In general, with respect to an

entity and to the context/role under which the interaction took place, the NoR received for each MFV is stored. These values are categorized according to: context/role, MF and MFV (see Figure 4.2).

- (a) *Non-Repudiation*: since ratings can be only given following a transaction, neither party can repudiate the ratings concerning it;
  - (b) *Aggregation*. In the *e-commerce/seller* context/role, as a result of a rating, the NoR of the corresponding MFV is increased by 1. For instance, if a buyer assigns *poor* to the *Cheapness* of an online store, the NoR of the MFV *poor* related to the MF *Cheapness* is increased by 1 (see the dashed boxes in Figure 4.2). In this way we avoid to aggregate inhomogeneous information. In the *e-commerce/buyer* context/role, following a rating the value of the MF *Reliability* is updated by increasing by 1 the total number of transactions and recalculating the average amount.
  - (c) *History*. The history can be managed by storing the time in which a rating is expressed. As time passes, the past ratings may need to be aggregated. In this case, in the *e-commerce/seller* context/role, the aggregation of the values of the MF is obtained by adding the NoR of the corresponding MFV.  
In the *e-commerce/buyer* context/role, the history is managed similarly with the only difference that the aggregation of the values of the *reliability* of the buyer is obtained by adding the total number of transactions and then re-calculating the average;
  - (d) *Aging*. The oldest information should be given less importance than the most recent. Who uses it should decide how to weight it (*dynamic and subjective properties*);
4. *Information Sharing*. All users, without distinction, can access to the same information (*Democracy*). Only the average amount spent, used to measure the *Reliability* of the buyer, is published, while the number of transactions is kept confidential. Furthermore:
- (a) *Knowledge*. To interpret and manage the information shared by the system it is sufficient to know how the data are stored (Figure4.2);

- (b) *Clarity*. The information is evidently easy to understand;
  - (c) *Usability*. The user is required to make an assessment on the interaction by simply choosing values from lists;
  - (d) *Untraceability*. The ratings are stored as described in point 3. Therefore it is not possible to identify the raters;
5. *Recommendation System*. This model is only concerned with gathering, aggregating, storing and sharing ratings without including a Recommendation System. At the same time, however, the ratings expressed on the past behavior of users (*indirect trust*) are made available divided into two contexts/roles. This enables an easy build of a custom Recommendation System (*subjective property*) effective to identify the right entities to interact with in a given situation (*propagative property*). Moreover, as already mentioned, the user's private information may also be managed by means of the trust-chains (*direct trust*). We believe that the *Recommendation System* in its decision-making process should ensure that:
- the recent *positive ratings* should have low impact on reputation (*reputation lag*);
  - even a single recent *negative rating* has a strong impact on reputation (*event sensitive*);
6. *Incentive Mechanism*. We adopt the incentive mechanisms based on financial rewards presented in [76]. In addition, dishonest users are discouraged, as shown in the following.
7. *Malicious Attacks Resilience*. The aim of our model is to make the user aware of the history of the counterpart: it will be the user, in a subjective way, to decide how much trust to place in it from time to time. Particular attention must be paid to the way in which the reliability of the buyer is handled. Firstly, we highlight that the transactions always have a cost: that of the purchased good/service. Therefore, a buyer who wants to increase his reputation maliciously should carry out transactions spending a lot of money.

This is a pretty strong disincentive that protects the system from many attacks. Another technique might perform a behavioral analysis to identify users who make many low value transactions.

In line with some consolidated solutions [56, 72, 109], we can deduce that the effectiveness of the following attacks is reduced for the following reasons:

- (a) *Whitewash* and *Sybil Attacks*: newcomers are not assigned any initial value, therefore who interacts with a newcomer will be aware of this and will be able to take all the necessary precautions.
- (b) *Traitor*: the number of ratings with negative values will be known to the users, thus the objective of the attacker will be nullified.
- (c) *Fake transaction*, *Promote*, *Ballot stuffing* and *Exit*: the danger of attack is severely curtailed from the application of mechanisms to discourage dishonest behavior. Furthermore a rating can only be expressed only as a result of a transaction, whose cost discourages malicious user to make fake transactions.
- (d) *Slander*: if an entity receives a lot of negative ratings from newcomers it would understand it is under attack and would avoid future interactions with them. In addition, the same mechanism of *Promote* is also effective in this case.
- (e) *Slander+Promote*, *Self-promote*, *Oscillation* and *RepTrap*: being curtailed the danger of *Slander* and of *Promote*, a simultaneous attack is not very effective as well.
- (f) *DOS*: the system for the management of the ratings must provide mechanisms (e.g. the use of message queues and/or of a decentralized system) to handle the sudden increase in requests.
- (g) *Context/Role Sliding*: this threat is avoided by maintaining separate transactions for contexts/roles;
- (h) *Orchestrated*: by limiting all of the above threats, this threat is limited too.

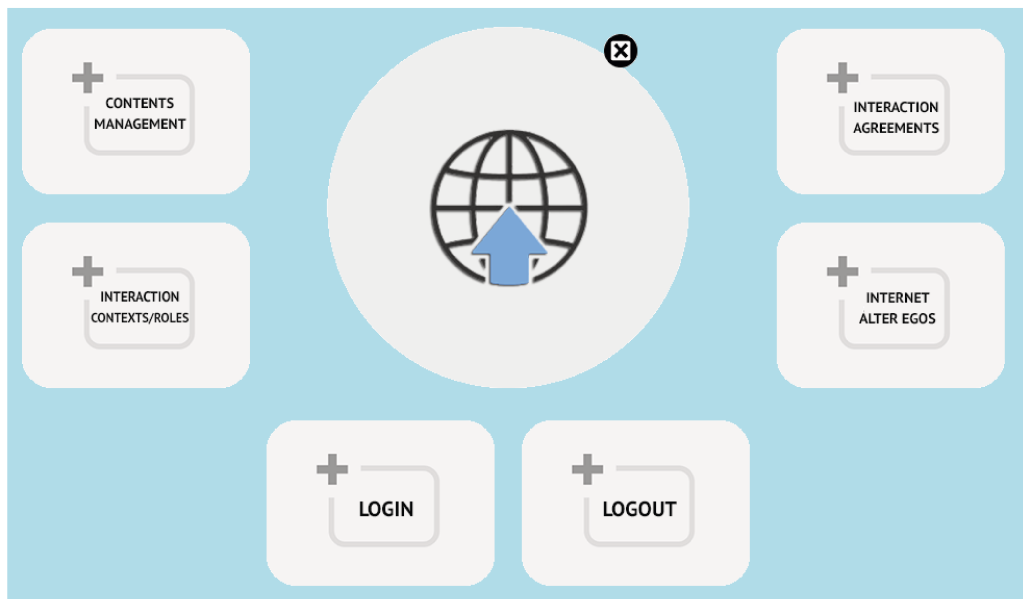
# Chapter 5

## Scenarios of the Trust Ecosystem

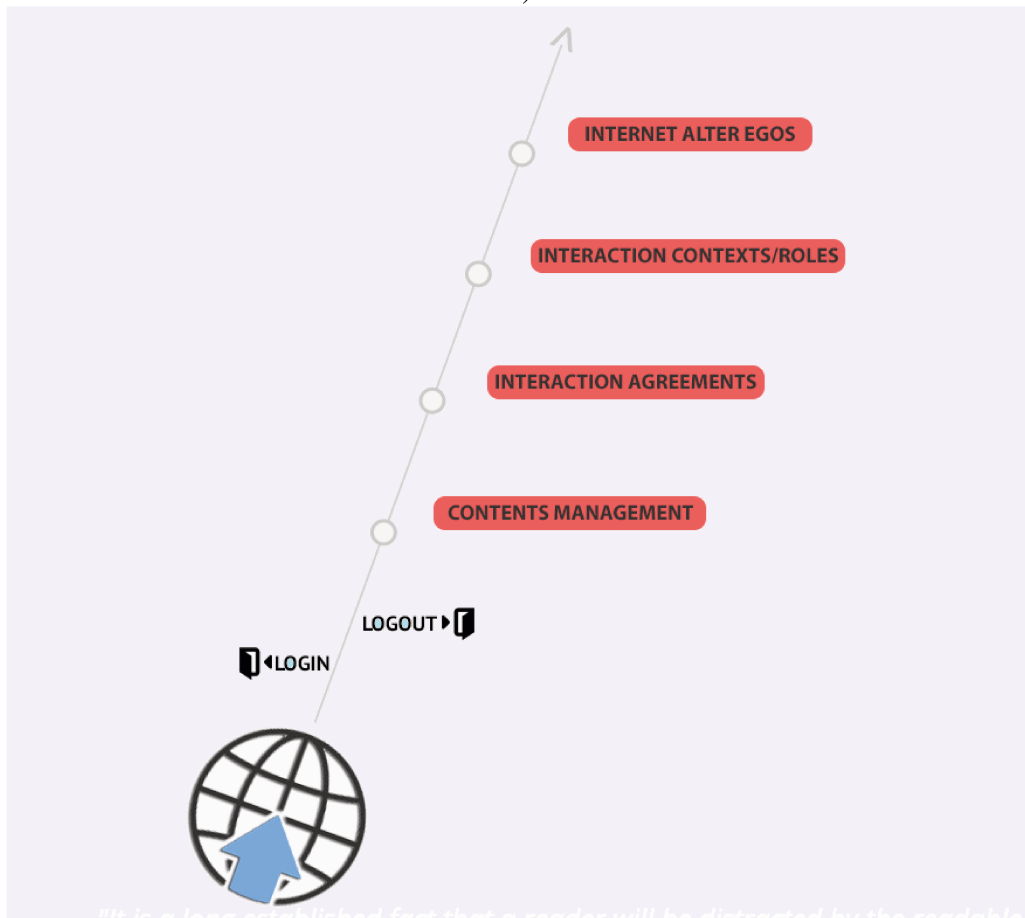
In this chapter we will describe some of the scenarios that can make clear advantages, ease of use and potentiality of the Trust Ecosystem (TEco). In the first three scenarios we will show the backend of the accreditation process to the TEco, Single Sign-On (SSO) and the management of Internet Alter Egos (IAEs) by the user. Following, we will describe some situations arising in the current Internet, showing how they would developed in the TEco, and how some of the issues described in the previous sections would find solution or would not occur at all.

In the description of the scenarios we will assume that the user device is equipped with a software called *TEco-Console*, which allows him/her to establish inter pares interactions in the TEco. It also allows the user to manage all information concerning him/her and greatly simplifies the user experience compared to the current Internet/Web as we will show through some GUIs. The *TEco-Console*, also thanks to the Internet Agent present within it, assists the user in the management of his/her own IAEs, in the login/logout through the SSO, in the visualization of the standard Interaction Contexts/Roles (ICRs), etc. In particular, the Internet Agent, based on experience, suggests the most appropriate ICR and IAE in all circumstances. The *TEco-Console* can be launched traditionally through an O.S. command. Nevertheless, it could also be launched through a specific key on the keyboard (e.g., a completely new key or a Function Key, see Figure 5.2). Figure 5.1 shows two possible versions of its main interface.

Furthermore it is assumed that browsers are compatible with the TEco, i.e.,



a)







b)




Figure 5.1: Main interface of the TEco-Console.



Figure 5.2: TEco key.

that they are equipped with a special plugin able to interact with the Internet Agent and to move the interaction in the TEco also during normal web browsing. In fact, thanks to the plugin, the browser address bar shows the icon  that allows to instantly load the appropriate GUI of the *TEco-Console* (see Figure 5.3) from which user can directly select the IAE and the ICR to bring the interaction in the TEco.

When an interaction in the TEco is established, the address bar also shows the IAE icon selected by user (e.g. ) , the counterparty's IAE icon (e.g. ) and  that indicates the Inter Pares Interaction (see Figure 5.4).

By clicking on the IAE's icon, a window showing information related to the IAE is displayed. An example of this is shown in Figure 5.5. The figure shows the window of the IAE's properties  divided into three sections: *IAE info*, *Reputation info* e *Reputation view*. In the first one, IAE's attributes are listed. Certified attributes are characterized by the icon . The *Reputation info* section shows all the information about the IAE's reputation  in the ICR *e-commerce/buyer* with the associated *Main Features*. For all *Main FeaturesValues* the number of ratings received by the IAE is reported (see section 4.2). The *Reputation view* section reports the reputation of the selected IAE.

In the future, it will be possible to know the reputation of an entity in the TEco according to the ratings received (for a detailed explanation on this aspect see Section 4). The user can decide whether to take the interaction in the TEco, by clicking on the button "*TEco In*" or to interact in the current Web, by clicking on

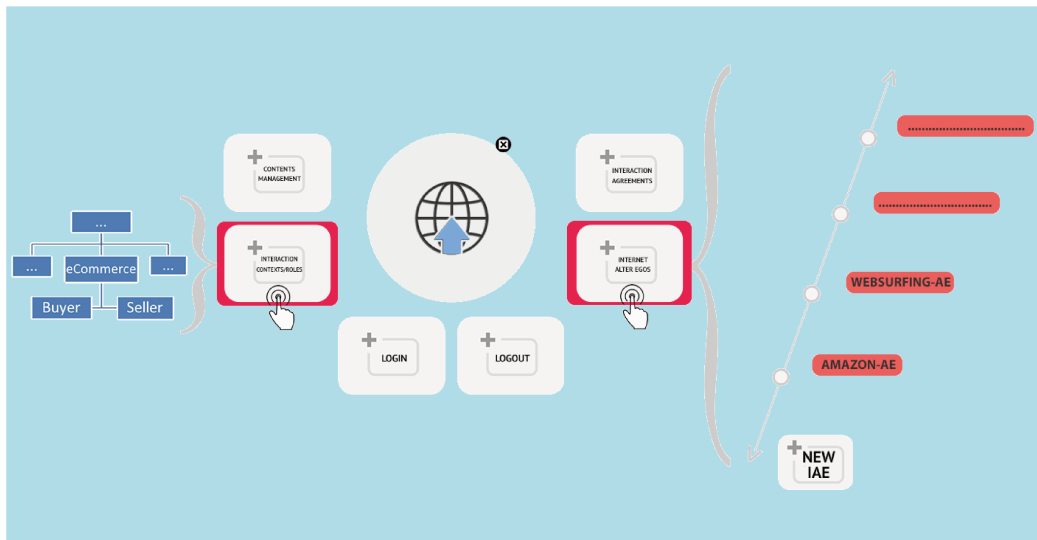


Figure 5.3: Selection of the IAE and the ICR for a TEco Inter Pares Interaction.



Figure 5.4: Browser with TEco interactions' icons.



the button “*TEco Out*” or by closing the window. The buttons “*TEco In*” and “*TEco Out*” are present both in the *TEco-Console* (see Figure 5.3) and in the window of the relying party’s properties (see Figure 5.5).

By clicking on “*TEco In*” the agent sends to the relying party the request of interaction together with the Alter ego and the Agreement chosen by the user. To establish interaction in the TEco the agents exchange various details (as shown in section 3.3) that have not been reported in the described scenarios because they are hidden from the user. In general, the Website interfaces are the same both in the TEco and in the current Web. Nonetheless, some websites can also provide specific interfaces for TEco users. For instance, websites may omit login masks, password recover and Captcha controls [2], they could offer new and innovative services reserved only to them.

## 5.1 Scenario 1: TEco accreditation.

*In this scenario is shown how to manage own digital identity in the TEco.*

In the TEco each user owns a Trusted Digital Identity (TId) managed by an Identity Management system (the reference IdM) which, among other things, keeps the references to all the data that “belong” to the user (e.g. attributes). In addition, through the Content Management Framework, the reference IdM manages all content produced by the user. In this way, the digital identity is not fragmented and the user always can trace all the data concerning him/her. Below we describe how a natural person, Bob, can get his own TId using the “*TEco accreditation*” process (see Figure 5.6).

1. Bob contacts one of the IdMs adhering to the TEco and asks for accreditation;
2. The IdM, through the form shown in Figure 5.7, asks Bob to choose the credentials to access the TEco. The IdM decides the type of credentials to provide (e.g. username/password, biometric data, etc.) by adapting its security standards to new technologies over time;

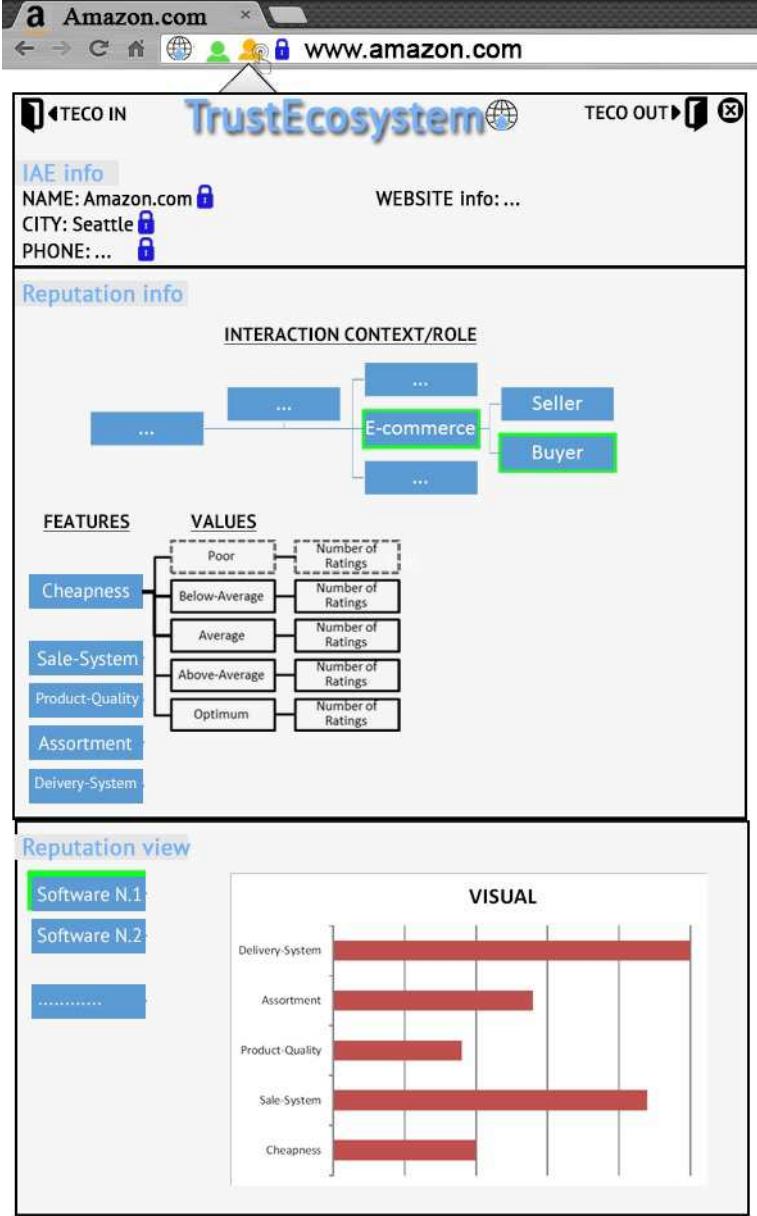


Figure 5.5: Information about an IAE in the TEco.

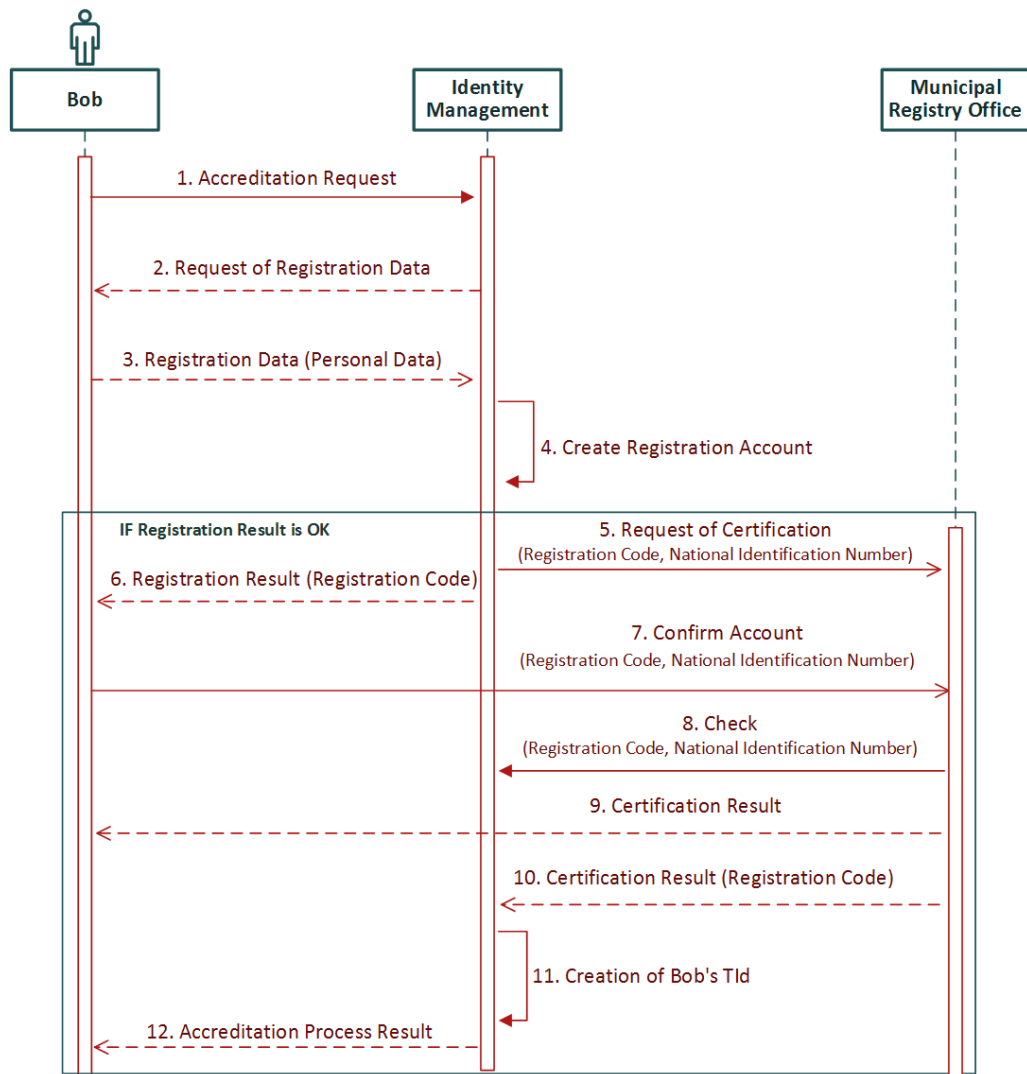


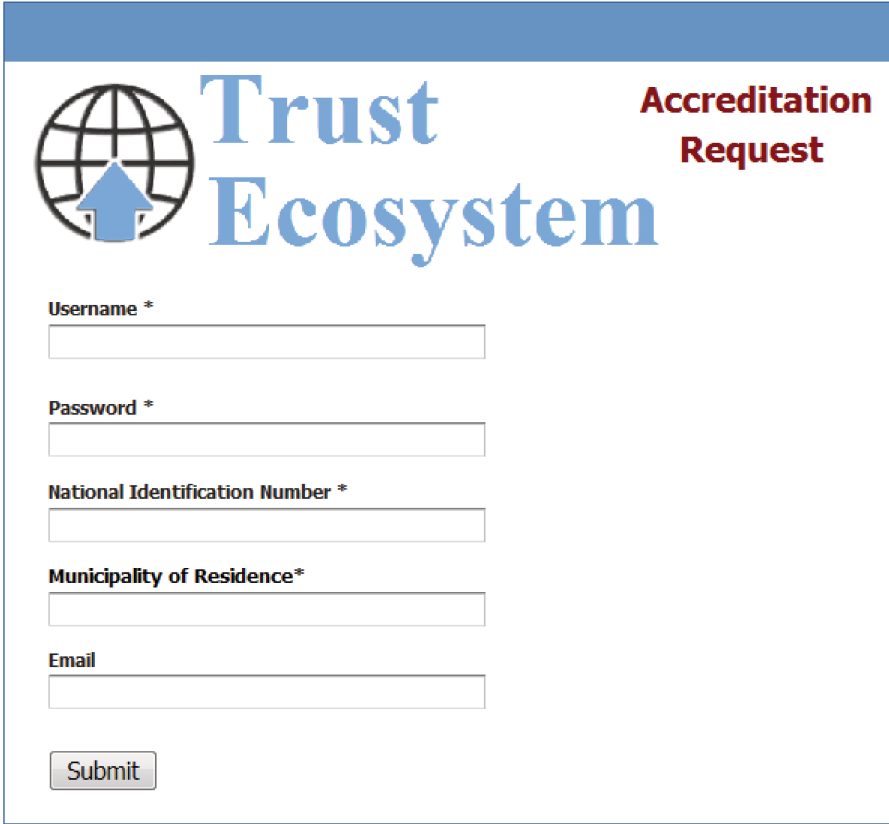
Figure 5.6: TEco accreditation sequence.

3. Bob sends *access credentials*, its own *national identification number*, *city of residence* and an *email address* to the IdM;
4. The IdM creates a registration account to the TEco that, however, will not allow the user to access until it will be certified;
5. The IdM requires the certification of Bob's identity to the Municipal Registry Office of his city. To this extent, it sends him the pair (*RegistrationCode*, *national identification number*);
6. The IdM provides Bob with the result of the request sending him a *RegistrationCode* that uniquely identifies the request;
7. As soon as possible, Bob must go, with an ID document, to the Municipal Registry Office in order to confirm the registration associated with the pair (*RegistrationCode*, *national identification number*);
8. The Municipal Registry Office checks if the *national identification number* indicated in the registration request belongs to Bob. If the data is correct the registration will be certified, otherwise it will be canceled;
9. The Municipal Registry Office tells Bob the verification result;
10. The Municipal Registry Office tells the IdM the outcome of registration verification with its *RegistrationCode*;
11. The IdM creates the Bob's Trusted Digital Identity;
12. The IdM communicates the result of accreditation to the TEco process to Bob becoming its *reference IdM*.

From now on, Bob owns a TId and will have access to the TEco as shown in Scenario 5.2.

## 5.2 Scenario 2: Single Sign-On in the TEco

*This scenario show the Single Sign-On in the TEco.*



The image shows a web form for an accreditation request. At the top left is a logo consisting of a globe with a blue house icon inside. To the right of the logo, the text "Trust Ecosystem" is written in a large blue serif font. Further to the right, the words "Accreditation Request" are written in a smaller, bold, dark red sans-serif font. Below the logo and title, there are five input fields, each with a label and an asterisk indicating it is required: "Username \*", "Password \*", "National Identification Number \*", "Municipality of Residence\*", and "Email". Each label is positioned above its corresponding text input box. At the bottom left of the form area is a grey "Submit" button.

Figure 5.7: TEco accreditation request.

The image shows a web interface for 'Trust Ecosystem' with a 'Single Sign-on' section. On the left, there is a logo consisting of a globe with a blue house icon inside. To the right of the logo, the text 'Trust Ecosystem' is displayed in a large blue font, and 'Single Sign-on' is in a smaller red font. Below the logo and text, there are two input fields: 'Username \*' and 'Password \*'. A 'Submit' button is located at the bottom right of the form area.

Figure 5.8: TEco Single Sign-on

A user with the TId to log in the TEco has to load the *TEco-Console* (e.g., using the *TEco-Key* as in Figure 5.2) that will require, through the GUI of Figure 5.8, to enter the credentials provided in the accreditation request. From now, to interact in the TEco (as in the current Internet) but, as we will see below (see Figure 5.14), a simple click to select an IAE will need.

Then the entity receives the list of all standardized Interaction Contexts/Roles and the list of all its own IAEs created till that time from the IdM. Then, s/he can manage her/his lists by *TEco-Console* as shown in the next scenario.

Login to the TEco lasts indefinitely even when the system is turned off. Therefore, the user must explicitly log out or link this action to a particular event: after a fixed period of time, when the system turns off, etc.

### 5.3 Scenario 3: Management of IAEs

*This scenario describes the creation and personalization of the IAEs according to user's needs.*

It is useful to remember that the *reference IdM* keeps the user's IAEs and when user accesses to the TEco the IAEs' local list is synchronized with remote ones.

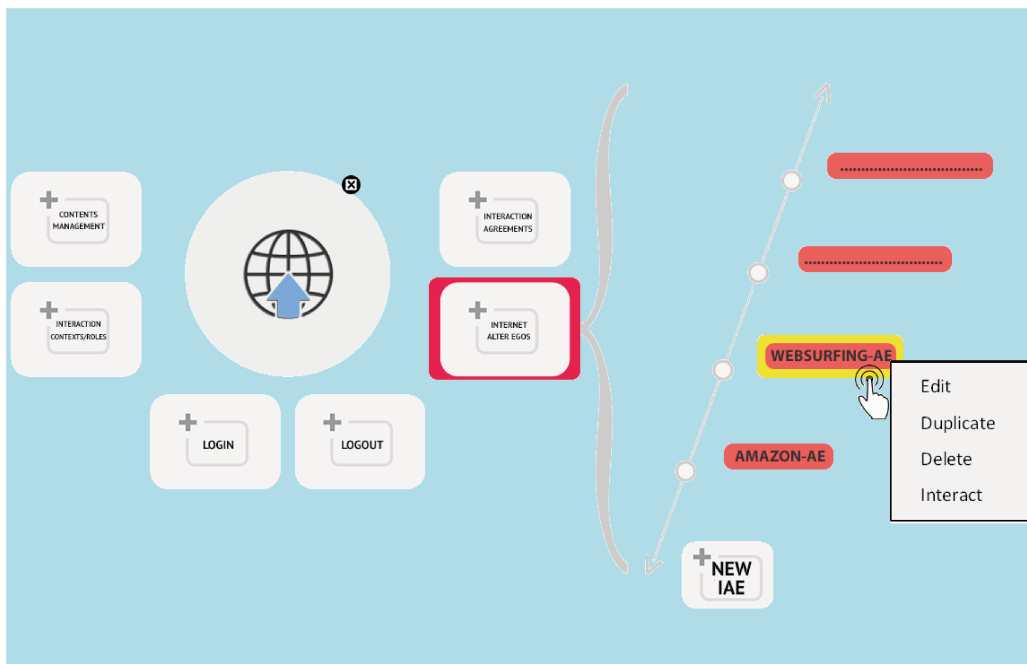


Figure 5.9: Management of IAEs with the TEco-Console.

After user is logged in the TEco, s/he can manage his/her IAEs using specific GUIs of the *TEco-Console* which will also handle their synchronization.

As we can see in Figure 5.9, by selecting the “*Internet Alter Egos*” option, the list of all alter egos is shown. The “+*New IAE*” button opens an interface (see Figure 5.10) that allows the user to create a new IAE at any time by choosing which information to include in IAE among those associated to his/her own TId (i.e. *Meta IAE*).

During IAE creation, the user can choose a default agreement by selecting it among the existing ones, or create a new one with a procedure similar to that used for IAE creation. Agreements and IAEs are stored separately because in this way it is possible to associate the same agreement to different IAEs. In addition, depending on his/her needs, the user can also change the default agreement associated with the IAE during the negotiation.

As shown in Figure 5.9, the user can delete, duplicate, or edit an IAE with a simple click. We can assume that providers will make available specific functionality to assist user in creating IAEs (see Scenario 5.7). In addition they may also



<b>IAE NAME:</b> <input type="text"/>		
<b>IAE DESCRIPTION:</b> <input type="text"/>		
<b>IAE ICON:</b> 		
ATTRIBUTES		
NAME	VALUE / URL OF VALUE	URL OF CERTIFIER
Default-IA	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/> 

Figure 5.10: Creation of a new Internet Alter Ego.

provide some predefined IAEs for generic interactions. When the relying party, e.g. a bank or an institutional office, already has the user's data, it could create an IAE and send it directly to him/her. In order to increase privacy and security, it can also restrict access and use of the IAEs by setting credentials (e.g., password, biometric data, etc.).

In addition, to simplify the management of the IAEs, each of them can be customized by setting some attributes like *name-IAE*, *IAE-description*, *IAE-icon*, etc.

It should be pointed out that the parties only exchange IAEs' temporary identifiers (i.e. *tempIAE*), while the permanent ones and the customization data (e.g. *IAE-name*, *IAE-description*, *IAE-icon*, etc.), for security and privacy reasons, are never revealed to the relying parties. Actually, IAEs' permanent identifiers are even unknown to the owners as they only receive periodically generated temporary identifiers by IDMs (see Section 3.2).

## 5.4 Scenario 4: Web surfing

*This scenario illustrates how a user can establish an interaction in the TEco while surfing the Web without additional efforts and with indisputable advantages. It has been chosen to show the interaction*



IAE NAME: <i>WebSurfing-AE</i>		
ATTRIBUTES		
NAME	VALUE / URL OF VALUE	URL OF CERTIFIER
Nickname	Bobby	
Default-IA	WebSurfing-IA	

INTERACTION AGREEMENT: <i>WebSurfing-IA</i>	
TERM	VALUE
ICR	Website/Surfer
ICR-RelyParty	Website/Owner
Privacy Level	High
...	...

Figure 5.11: An Alter Ego and an Agreement to surf the Web.

*from the user's viewpoint, omitting communication details between the Internet Agents. It is assumed that the user has already logged in the TEco.*

As we have seen, the use of IAEs in the TEco allows users to decide what personal information to share with other parts. In this case, to surf the Web using the TEco, Bob created a specific IAE named *WebSurfing-AE* and, to maintain the complete anonymity, only provided the nickname *Bobby*. In addition, he created an agreement in which included the *term Website/Surfer* as his ICR and *Website/Owner* as counterparties' ICR as well as the *term "Privacy level: High"* to impose on the counterparties to respect his privacy and anonymity. To this extent, counterparties can not ask private information in addition to those included in the IAE (see Figure 5.11). Thus, Bob can use the TEco and continue to surf the Web in the same manner as he usually does with the only addition of choosing an IAE. In practice, Bob:

1. opens the browser;

<b>IAE NAME: <i>WebOwner-AE</i></b>		
<b>ATTRIBUTES</b>		
<b>NAME</b>	<b>VALUE / URL OF VALUE</b>	<b>URL OF CERTIFIER</b>
Nickname	TheNyTimes	
Default-IA	<b><i>WebOwner-IA</i></b>	

<b>INTERACTION AGREEMENT: <i>WebOwner-IA</i></b>	
<b>TERM</b>	<b>VALUE</b>
ICR	Website/Owner
ICR-RelyParty	Website/Surfer
Privacy Level	High
...	...

Figure 5.12: An Alter Ego and an Agreement of a website.



Figure 5.13: Browser with the TEco's icon.

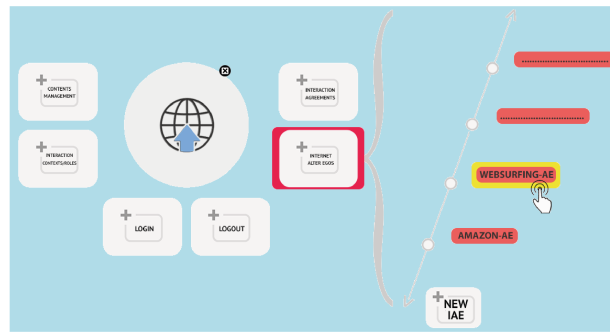


Figure 5.14: Selecting an IAE.



Figure 5.15: Browser with Bob's IAE icon.




2. runs the *TEco-Console* by clicking on the icon  shown in the browser address bar (see Figure 5.13) or by the *TEco-Key* (see Figure 5.2);
3. selects the IAE *WebSurfing-AE* (see Figure 5.14). As you can see in Figure 5.15, to indicate the chosen IAE in the browser address bar the icon  is shown;
4. types the website URL (e.g. *www.nytimes.com*);
5. clicking on the icon  in the address bar (see Figure 5.16) information about the relying party is displayed (see Figure 5.5). In the section *Reputation-Info* and *Reputation-View* Bob can inspect the reputation of the relying party and decide whether to continue the interaction with him/her. Otherwise, if the reputation is not considered sufficient, Bob can search a website with a reputation that meets his expectations (e.g., by typing a new URL in the browser, using a search engine, etc.).



Figure 5.16: Browser with entities' icons.



Figure 5.17: Browser with entities' icons and Inter Pares interaction's icon.

6. if he decides to continue the interaction in the TEco Bob must click on the *TEco-In* button (see Figure 5.5). Then the Internet Agent will establish Inter Pares Interaction in the TEco and in particular it will send the relying party the IAE *WebSurfing-AE* and the agreement associated with it (i.e. *WebsiteSurfer-IA* in Figure 5.11). But if Bob wants to continue the interaction in the Web out of the TEco he can click on the *TEco-Out* button or simply close the window;
7. as it can be seen in Figures 5.11 and 5.12 the agreements of each party satisfy the mutual requests: *website/surfer*, *website/owner* and *high level of privacy*. Therefore, the respective agents agree, independently and without the need for outside intervention, an Interaction Negotiated Agreement (NIA), which in this case is in the Bob's agreement;
8. From now on, Bob can consult the website knowing that underlying the interaction there is a negotiated agreement that binds the provider to maintain a high level of privacy (see Figure 5.17). In addition, the provider can not deviate from the provisions in the negotiated agreement so, for example, it can not claim payments without a redefinition of the NIA since it is not explicitly agreed.

At the end of the interaction, the parties can give their ratings sending feedbacks like described in the Section 5.6 .

## 5.5 Scenario 5: Negotiated Interaction Agreement

*This scenario describes an interaction in the TEco between a teacher who gives online lessons and a student. It also shows the negotiation phase of the agreement. It is assumed that both users have already logged in the TEco.*

IAE NAME: <i>Teacher-AE</i>		
ATTRIBUTES		
NAME	VALUE / URL OF VALUE	URL OF CERTIFIER
Nickname	Prof. Mario	
Default-IA	Teacher-IA	
City	Salerno	<i>www.comune.salerno.it</i> *
Profession	Full professor	<i>www.miur.it</i> **
Subject	Software Engineer	<i>www.miur.it</i> **

\* Municipal Registry Office of Salerno

\*\* Ministry of Education, Universities, and Research (MIUR)

INTERACTION AGREEMENT: <i>Teacher-IA</i>	
TERM	VALUE
ICR	eLearning:SoftwareEngineer/Teacher
ICR-RelyParty	eLearning:SoftwareEngineer/Student
Service Cost	50€/hour
Accepted payment methods	Advance payment
...	...

Figure 5.18: Alter Ego of Teacher Mario and his agreement.

Prof. Mario, through an interaction in the TEco, signed up for an advertising website to express his availability to give online lessons about *software engineering* using the alter ego *Teacher-AE*. He linked an *agreement* to that IAE in which he included the *terms* “**Service Cost: 50€/hour**” to indicate the hourly cost of the lessons and “**Accepted payment methods: advance payment**” to request advance payment of his lessons (see Figure 5.18). Alice is a student interested in receiving online lessons about *software engineering*.

1. Using the alter ego and the agreement represented in Figure 5.19 Alice makes some online research and find the following advertisement: “*Prof. Mario - Salerno (Italy), professor of software engineering, gives online lessons at the cost 50€/hour*” (see Figure 5.20).
2. Alice decides to click on the link of the advertisement that redirects her to *prof. Mario*’s web page (see Figure 5.21 );
3. Alice contacts prof. Mario clicking on the button “*Contact*”;

IAE NAME: <i>Student-AE</i>		
ATTRIBUTES		
NAME	VALUE / URL OF VALUE	URL OF CERTIFIER
Nickname	Alice	
Default-IA	Student -IA	
Subject	Software Engineer	

INTERACTION AGREEMENT: <i>Student-IA</i>	
TERM	VALUE
ICR	eLearning:SoftwareEngineer/Student
ICR-RelyParty	eLearning:SoftwareEngineer/Teacher
Service Cost	40€/hour
Service Subject	Lesson about Software Engineer
...	...

Figure 5.19: Alice's IAE and her agreement.

## SOFTWARE ENGINEERING TUTORING

**Prof. Mario – Professor of software engineering  
Salerno (Italy)  
Gives online lessons at the cost 50€/hour**

374 comments

Figure 5.20: Teacher's advertisement.

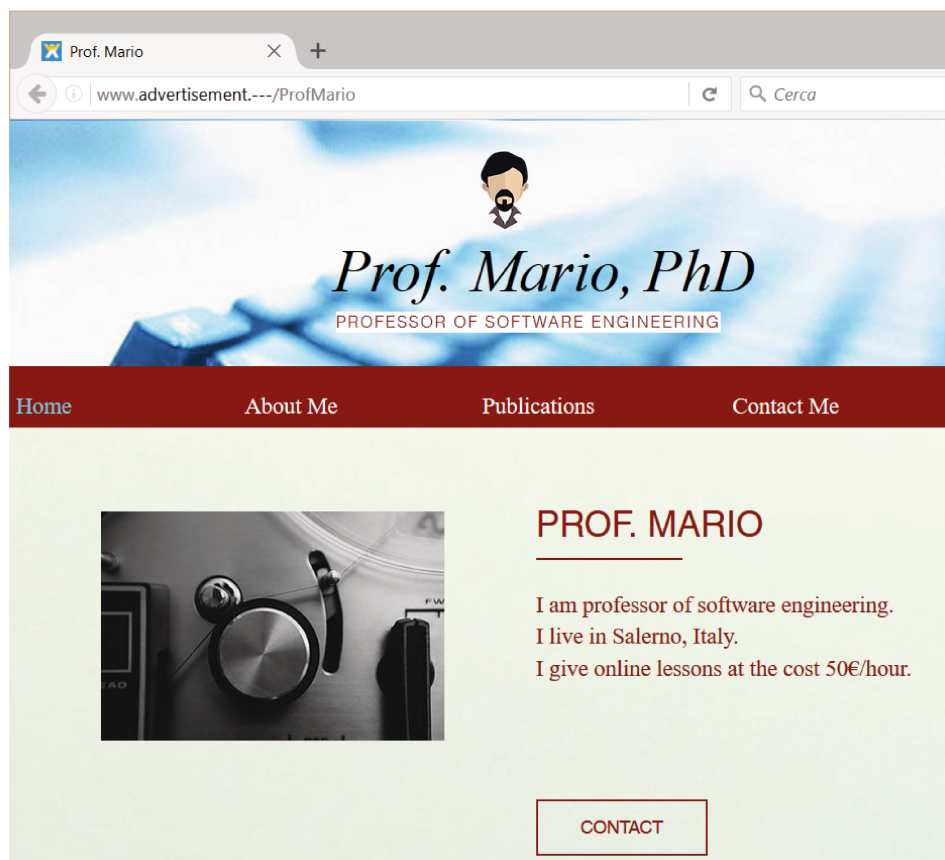


Figure 5.21: Teacher's website.



Figure 5.22: Notification of a TEco interaction request.

4. Alice's agent sends the alter ego and agreement to the prof. Mario's agent;
5. Alice's request for interaction in the TEco is notified to prof. Mario, possibly with a sound signal, as in Figure 5.22;
6. Prof. Mario clicks on the "Details" button in Figure 5.22 to display information related to the request (see Figure 5.23). Since prof. Mario requires an advance payment for his lessons, he is not interested in knowing the reputation of the relying party. But he notes that in her agreement Alice said she wants to pay 40€/hour for the lessons, in spite of 50€/hour he requested. Because he is willing to accept at least 45€/hour, he changes the agreement as shown in Figure 5.23 and accepts the interaction request by clicking on the "Accept" button. The agent sends Alice the alter ego *Teacher-AE* and the agreement associated with it (see Figure 5.18) with the term "**Service Cost: 45€/hour**";
7. After she received the acceptance, Alice can display of the **prof. Mario's** reputation and the agreement by clicking the button "Details" (see Figure



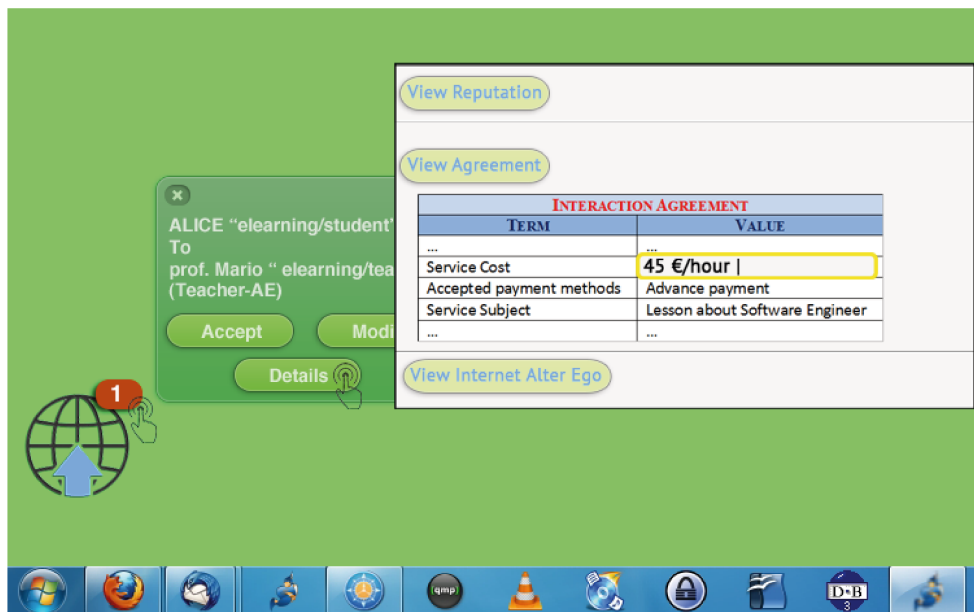


Figure 5.23: Details of the notification.

5.24);

8. Alice is satisfied of the reputation of “*prof. Mario*” but she notes that in the agreement the required cost of lessons is 45€/hour (shown in red in Figure 5.24) in spite of 40€/hour she had communicated. However, she decides to accept the interaction by clicking on the button “*Accept*”. Her agent sends to *prof. Mario* the notification of acceptance of the last agreement received which becomes the official Interaction Negotiated Agreement (NIA);
9. From now on, since the interaction has been established in the TEco, Alice pays for lessons (e.g. for an hour) and *prof. Mario* gives his prepaid lessons in Software Engineering;
10. At the end of the lessons, they both can express an opinion (i.e. rating) on the other party by sending feedback to their own *Reference RMS* as we will explain in the next scenario.

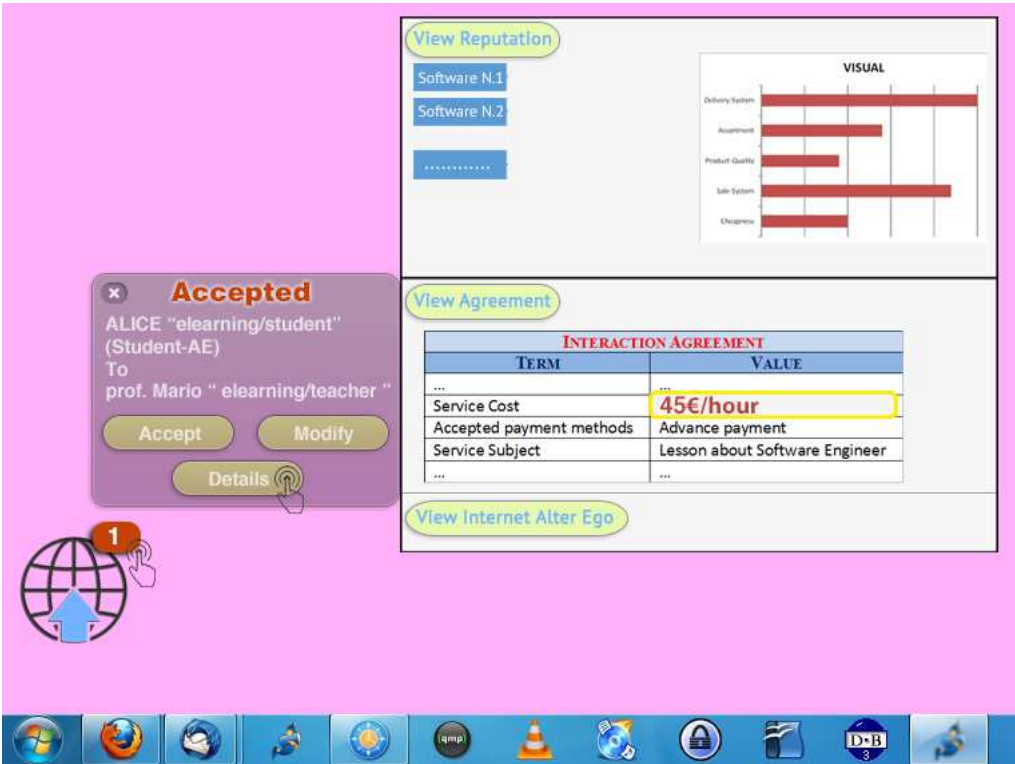


Figure 5.24: Notification of a TEco interaction acceptance with details.

<b>IAE NAME: <i>Amazon-AE</i></b>		
<b>ATTRIBUTES</b>		
<b>NAME</b>	<b>VALUE / URL OF VALUE</b>	<b>URL OF CERTIFIER</b>
Nickname	Bobby	
Default-IA	Amazon-IA	
Address	Condotti street, Rome	
Default-URL	amazon.com	

<b>INTERACTION AGREEMENT: <i>Amazon-IA</i></b>	
<b>TERM</b>	<b>VALUE</b>
ICR	ecommerce/buyer
ICR-RelyParty	ecommerce/seller
Maximum amount	100€
Payment methods	Credit card
Credit Card	9999-2222-0000-1111
...	...

Figure 5.25: Bob's IAE named *Amazon-AE*

## 5.6 Scenario 6: InterPares Interactions

*This scenario describes some interactions of a user who wants to shop on several e-commerce websites in the TEco. It is supposed that the user has already logged in the TEco.*

### Buying on Amazon.com

We suppose that Bob has made several purchases in the past from a seller for whom he has a great trust level (e.g., Amazon.com). In the TEco he can speed up the interaction by creating a specific alter ego (e.g., *Amazon-AE*) and associating an agreement with it (see Figure 5.25).

In this way, Bob can shop on Amazon by simply opening the browser and typing its url "*www.amazon.com*". His Internet Agent associates this url with default one of *Amazon-AE* alter ego. Thus, it sends to Amazon the request to interact in the TEco with alter ego *Amazon-AE* and its associated agreement. Since Bob's agree-

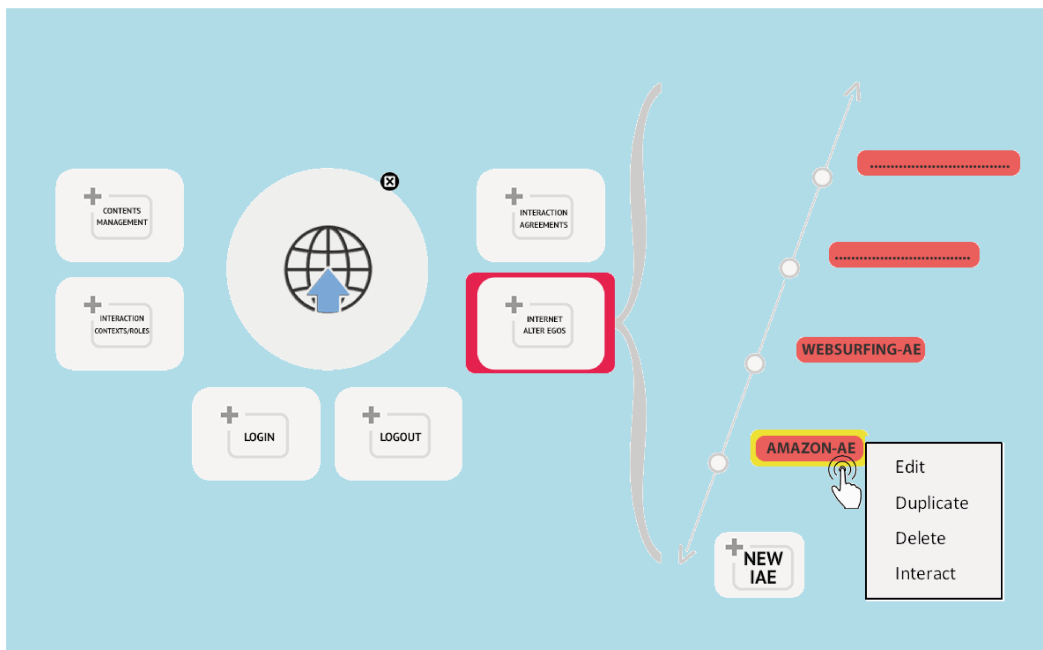


Figure 5.26: Duplication of an IAE.

ment is compatible with Amazon's *standard* one, their agents autonomously agree the negotiated agreement. Bob's agent sends to his *Reference RMS* the couple  $(tempAmazon; ecommerce/seller)$  and receives the Interaction Token with which he can identify the interaction with Amazon. Amazon's agent, in turn, sends the couple  $(tempBob; ecommerce/buyer)$  and receives the related token.  $tempAmazon$  and  $tempBob$  are related temporary identifiers received from their respective agents during the negotiation phase (see Section 3.3).

Bob is notified that the interaction with Amazon is in the TEco through the presence of the icons of the TEco displayed in the browser address bar, as shown in Figure 5.17. Otherwise, Bob can request the same interaction by double clicking on the IAE *Amazon-AE* from the *TEco-Console*. The agent will open the browser and access to the url "*www.amazon.com*" requiring an interaction in the TEco.

In either case, Bob does not evaluate the reputation of Amazon again because he has great trust in it. Therefore he can only select the desired products and confirm the purchase. It will be the agent, requiring the intervention of Bob only if necessary, which will handle the payment, set the shipping address etc. following


**Trust Ecosystem**

## Interaction Feedback

	Poor	Below-Average	Average	Above-Average	Optimum
Cheapness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Sale-System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product-Quality	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Assortment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Delivery-System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 5.27: Interaction feedback.

the indications set in the IAE and in the agreement.

As shown in Figure 5.27, at the end of the interaction and within the time-limit set by Bob's *reference RMS*, Bob's agent will ask him to express his own evaluation on selling limited to the interaction ICR (i.e. ecommerce/seller). The agent will send the values expressed by Bob as feedback to his *reference RMS* using the interaction token received before starting the interaction. Amazon's agent, instead, will automatically assign to the *Reliability* of Bob the amount of the transaction and will send it as feedback to its *reference RMS* using the interaction token.

### Buying on Trustworthy website

In the above described case, we saw that it is possible to have a dedicated IAE to interact with a particular seller in the TEco. However it is not needed a different IAE for each counterpart. Indeed, as we will show in this scenario, a single IAE can be used to interact with different counterparts.

We suppose that Bob in the past has made several purchases from sellers for whom he has a great trust level (e.g. ebay.com). Therefore he decided to create a dedicated IAE in order to use to interact with those sellers.

Using the *TEco-Console* Bob: duplicates *Amazon-AE* (see Figure 5.26), re-

<b>IAE NAME: <i>TrustworthyEcommerce-AE</i></b>		
<b>ATTRIBUTES</b>		
<b>NAME</b>	<b>VALUE / URL OF VALUE</b>	<b>URL OF CERTIFIER</b>
Nickname	Bobby	
Default-IA	Amazon-IA	
Address	Condotti street, Rome	

<b>INTERACTION AGREEMENT: <i>Amazon-IA</i></b>	
<b>TERM</b>	<b>VALUE</b>
ICR	ecommerce/buyer
ICR-RelyParty	ecommerce/seller
Maximum amount	100€
Payment methods	Credit card
Credit Card	9999-2222-0000-1111
...	...

Figure 5.28: Bob's IAE named *TrustworthyEcommerce-AE*.

names it in *TrustworthyEcommerce-AE* (see Figure 5.28), leaves the same Default-IA (i.e. *Amazon-IA*) and does not set any default url.

When Bob wants to shop on a trusted seller (e.g. eBay), he can do the following:

1. open the browser and types the url "*www.ebay.com*";
2. run the *TEco-Console*;
3. his agent highlights the IAE *TrustworthyEcommerce-AE* with the ICR *ecommerce/seller* it has already used in the previous interactions with eBay;
4. click on *TEco-In* button in order to confirm the suggestions of his agent who will require an Inter Pares Interaction to eBay.

Otherwise, Bob can:

1. run the *TEco-Console*;

2. double-click on the IAE *TrustworthyEcommerce-AE* and type the URL *www.ebay.com* in the browser address bar since the agent will require an Inter Pares Interaction.

As we can see, this is the same scenario of *Buying on Amazon.com* except for the second case in which Bob must type the url in the browser.

## 5.7 Scenario 7: TEco Inter Pares Interactions with Banks and Institutions

*This scenario describes how new attributes created by organizations and/or institutions are associated with the TId. Moreover, it is also shown how in some cases, for example in the case of a bank, a predefined IAE is sent to the entity. It is supposed that the user has already logged in the TEco.*

### **New attributes produced by institutions.**

We suppose that Bob obtains the PhD in Computer Science at the University of Salerno. Then, the University will send an interaction request in the TEco with the ICR *CertifiedData/Producer* to Bob. In this way, Bob can link his new degree in his certified attributes list. Later, when Bob will read the communication, he can accept or reject the University request.

Hence, Bob should only accept the request: it will be his agent to add the *PhD in Computer Science* into the certified attributes list of his *Meta IAE* linking the *University of Salerno* as certification institution. Bob's agent will send the notification of acceptance to the University indicating the ICR *CertifiedData/Consumer*.

### **Bank Account.**

We suppose that Bob opens an online bank account using an interaction in the TEco. So, the bank will be able to create and send the *reference IdM* of Bob a

specific IAE (e.g. *BankAccount-AE*) with only the strictly necessary data to allow him to manage his online account in the TEco. The *reference IdM* of Bob will update the list of all his IAEs.

Then, to access his online account, Bob can simply double-click on *Bank Account-AE* exactly as we described in the case of *Amazon-AE* (see Scenario 5.6).

This does not preclude Bob to create his IAE in order to interact with his bank. Moreover, as previously mentioned, for the use of this kind of IAE it may be necessary to set access credentials.



# Chapter 6

## Achievements and Future Research

In this PhD thesis, we discussed some critical issues related to the current Internet and we proposed an overall solution called Trust Ecosystem (TEco), which defines a trust area on the Internet, where users can freely move and safely interact with a greater degree of mutual trust. We also discussed how it can be implemented through the integration of some existing and new systems and how this enhances the current Internet without upheavals. In our Trust Ecosystem entities own a Trusted Digital Identity (TId) that allows their identification in a unique and certified way.

Thus, when in an interaction the entity is required to identify itself in a certified way, it can always choose whether or not to provide its data or give up with the interaction. However, in the TEco mutual identification is only required when it is absolutely necessary (e.g., online banking), while in all other cases, the essential or required information to establish an interaction will only be disclosed.

As we showed before, to establish an interaction and, in general, a communication between two entities it is not necessary that mutual identities are disclosed but it is enough providing their identifiers or aliases. To implement this principle we have introduced the Internet Alter Egos (IAEs) in the TEco because they enable communication between entities while maintaining an high level of privacy or the complete anonymity. The IAEs also transfer in the TEco (i.e. in the online world) the concept of “*multiple identities*” of the offline world. It is known, indeed, that each individual/company shows a different side/aspect of itself, i.e. an alter ego,

depending on the part with which it relates to. Each alter ego contributes to forming the identity of an individual/company. In addition, IAEs allow to expand the concept of privacy as, in addition to the protection of the only sensitive data, allow to decide what data to publish in any specific situation.

As we already showed, the Trust Ecosystem is very easy to use. Indeed, in section 5 we have seen some scenarios that highlight and make fully understand its advantages and potentiality. As we can guess, users will not be forced to drastically change the way they normally use both Internet services and Web browsing. Since the TEco does not require “upheaval” of the current Internet, it will be able to develop in parallel with it and, in any case, they can coexist.

Indeed, to simplify the user experience in the TEco it was introduced an Internet Agent which suggests or takes decisions on the basis of its acquired experience on entities and on the contexts/roles under which interactions take place. The agent helps the user in all situations. Thus the actions that the user must take are considerably reduced and, therefore, using services in the TEco will be simpler than on the current Internet.

In the TEco the entities are direct owners of the information they produce and they can decide which access rights to grant to other entities (e.g., reading, modification, deletion, duplication, disclosure, etc.). To this aim, it was introduced the Content Management Framework (CMF), which manages all the data related to the entities and ensures the rights set by the content owner, with any changes, are disclosed to the other entities and that they respect such rights. Another duty of the CMF is to “*certify*” with legal value the publication of a content on the Web.

Moreover, contrary to what occurs on the current Internet, in the TEco the users have equal bargaining power. Indeed, they can establish *inter pares* interactions tying counterparts to comply with specific and agreed conditions.

We also showed how entities, before establishing an interaction, can know reliable and updated reputation information about all users on the context/role under which the interaction takes place. In this manner entities can choose the counterpart that corresponds to their own needs and expectations based on the information obtained. Unfortunately current Trust and Reputation systems are confined within specific service providers and each of them collects different kinds of data emphasizing different features. Moreover, the way in which inhomogeneous values are

commonly aggregated is a critical point that it is not adequately investigated. This causes the impossibility to share information between existing Trust and Reputation systems. Instead, in the TEco, the limits of the current systems are exceeded because reputation data of entities can be used in all interactions and not only in a specific application domain.

Since the problems related to Trust and Reputation management are among the most urgent, thorny and controversial issues of the Internet, in this thesis we have paid special attention to them by addressing them in all their aspects. In addition, Trust and Reputation systems are also crucial for the purposes of the TEco since they are considered the only possible solution to assess the trustworthiness of users and reliability of information in online systems. However, as we shown before, currently the various Trust and Reputation systems are not standardized and, therefore, the trust and reputation information they manage can not be shared between different application domains and, often, it is not even reliable.

For this reason, we also defined a new meta model which simplifies and standardizes the definition of a generic Trust, Reputation and Recommendation (TRR) model. To this end, we identified the information that, in our opinion, needs to be provided in order to build a standard model. Based on this, we also proposed a pre-standardized TRR model for e-commerce and we listed some of the fundamental properties that must necessarily be taken into account in the construction of a TRR model. We additionally identified the peculiar characteristics (main features) that contribute to a greater extent to form the trust an entity in e-commerce context. Moreover, since the information on the main features is inhomogeneous, it has not been aggregated it in order not to undermine the significance of the results.

Another factor that may affect the reliability of a TRR model up to completely invalidate it is the vulnerability to malicious attacks. The main malicious attacks against a Trust and Reputation system were listed, and it was demonstrated the resistance of our model to them. Moreover, the collection and sharing of information is decoupled from that of the calculation of the trust/reputation. In this way, users can exploit different systems to derive the trust/reputation of an entity.

The work is still preliminary. In the future we will continue to work on Trust Ecosystem taking into account the contributions received by the scientific community. In addition, we will develop the communication protocols among all subsys-

tems and the formal languages to define the Agreement Terms and the Interaction Agreements. We will also implement a prototypical Internet Agent with a basic expertise to enable the testing of Trust Ecosystem.

Moreover, we will continue to work on the meta model and the Trust, Reputation and Recommendation model for e-commerce in order to achieve a standardization of them. In this regard, the meta model has been designed to be open to the contribution of the scientific community.

We are also trying to establish a Recommendation system for e-commerce that making use of information provided from our TRR model can help the user to make relatively better trust-based choices. In addition, more efforts are needed to define other standard TRR models for other contexts.

Lastly, we are working on the implementation of an environment for simulating and validating the proposed TRR models.

# References

- [1] Amazon. <http://www.amazon.com>.
- [2] CAPTCHA: Telling Humans and Computers Apart Automatically. Available online: <http://www.captcha.net>. Accessed: November, 2015.
- [3] COFACE - Confederation of Family Organisations in the European Union. Available online: <http://www.coface-eu.org>. Accessed: November, 2015.
- [4] Dropbox. <https://www.dropbox.com/>. Last accessed: February, 2016.
- [5] ebay. <http://www.ebay.com>. Accessed: February, 2016.
- [6] Facebook. <http://www.facebook.com>. Last accessed: February, 2016.
- [7] Google+. <https://plus.google.com/>. Last accessed: February, 2016.
- [8] Kantara Initiative. Available online: <http://www.kantarainitiative.org>. Accessed: October, 2015.
- [9] Liberty Alliance Project. Available online: <http://www.projectliberty.org>. Accessed: October, 2015.
- [10] Stackoverflow. <http://stackoverflow.com/>. Accessed: November, 2015.
- [11] Federated security: The shibboleth approach. Available online: <http://www.educause.edu/ero/article/federated-security-shibboleth-approach>, 2004. Accessed: October, 2015.

- 
- [12] ITU-T. NGN Identity Management Framework. Available online: <http://www.itu.int/rec/T-REC-Y.2720-200901-I>, 2009. Accessed: October, 2015.
- [13] Openid web page. Available online: <http://www.openid.net>, 2014.
- [14] J. Abendroth. *A Unified Access Control Mechanism*. PhD thesis, Trinity College Dublin, 2004.
- [15] A. Alkhalifah and J. D’Ambra. Identity management systems research: Frameworks, emergence, and future opportunities. *Identity*, 2015.
- [16] Alpar, G. and Hoepman, J.H. and Siljee, J. The identity crisis security, privacy and usability issues in identity management. *The Computer Research Repository (CoRR) 1101*, 2011.
- [17] D. Artz and Y. Gil. A survey of trust in computer science and the Semantic Web. *Web Semantics*, 5(2):pp. 58–71, 2007.
- [18] E. Bertino, F. Paci, and N. Shang. Digital identity protection - concepts and issues. *ARES ’09*, pages pp. lxix–lxxviii.
- [19] A. Bhargav-Spantzel, A.C. Squicciarini, and E. Bertino. Trust negotiation in identity management. *Security & Privacy, IEEE*, 5(2):pp. 55–63, March 2007.
- [20] H. Boley and E. Chang. Digital ecosystems: Principles and semantics. In *DEST ’07*, pages pp. 398–403.
- [21] Beat Bullying. #DeleteCyberbullying. <http://deletecyberbullying.eu>. Accessed: November, 2015.
- [22] S. Cantor et al. Assertions and Protocols for the Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 2005. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- [23] Y. Cao and L. Yang. A survey of identity management technology. *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*, pages pp. 287–293, Dec 2010.

- [24] E. Chang and M. West. Digital Ecosystems A Next Generation of the Collaborative Environment. *iiWAS '06*.
- [25] J.M. Chang, F. Chi-Chen, H. Kuan-Hsing, N. Kelly, W. Pei-Yuan, D. Yixiao, C. Chu, S. Gilbert, A.E. Kamal, and K. Sun-Yuan. Capturing cognitive fingerprints from keystroke dynamics. *IT Professional*, 15(4):pp. 24–28, July 2013.
- [26] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana. Social cloud computing: A vision for socially motivated resource sharing. *IEEE Transactions on Services Computing*, 5(4):pp. 551–563, Fourth 2012.
- [27] K. Chard, S. Caton, O. Rana, and K. Bubendorfer. Social cloud: Cloud computing in social networks. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pages pp. 99–106, July 2010.
- [28] European Commission. Cyberbullying risks permanent harm to European children. [http://europa.eu/epic/news/2014/20140805-cyberbullying-harm-european-children\\_en.htm](http://europa.eu/epic/news/2014/20140805-cyberbullying-harm-european-children_en.htm). Accessed: November, 2015.
- [29] European Commission. Digital Agenda for Europe. <http://ec.europa.eu/digital-agenda>. Accessed: November, 2015.
- [30] European Commission. Report on the Protection of Minors and Human Dignity Recommendations. [http://ec.europa.eu/archives/information\\_society/avpolicy/reg/minors/rec/2011\\_report](http://ec.europa.eu/archives/information_society/avpolicy/reg/minors/rec/2011_report). Accessed: November, 2015.
- [31] K. S. Cook, T. Yamagishi, C. Cheshire, R. Cooper, M. Matsuda, and R. Mashima. Trust building via risk taking: A cross-societal experiment. *Social Psychology Quarterly*, 68(2):pp. 121–142, 2005.
- [32] G. Costagliola, R. Esposito, V. Fuccella, and F. Gioviale. An architecture for user-centric identity, profiling and reputation services. *DMS 2009*, pages pp. 170–173.

- [33] G. Costagliola, V. Fuccella, and F. A. Pascuccio. Towards a Trust, Reputation and Recommendation Meta Model. *Journal of Visual Languages & Computing*, 25(6):pp. 850–857, 2014.
- [34] G. Costagliola, V. Fuccella, and F. A. Pascuccio. TEco: an integration model to augment the Web with a trust area for inter-pares interactions. In *The 21st International Conference on Distributed Multimedia Systems, Vancouver, Canada, August 31 - September 2, 2015.*, pages pp. 257–263, 2015.
- [35] Common Criteria. Common criteria for information technology security evaluation (cc-level eal7). Available online: <http://www.commoncriteriaportal.org/cc/>. Accessed: November, 2015.
- [36] M. Dabrowski and P. Pacyna. Generic and complete three-level identity management model. pages pp. 232–237, Aug 2008.
- [37] Z. Despotovic and K. Aberer. Possibilities for managing trust in p2p networks. Technical report, 2004.
- [38] A. Doan, R. Ramakrishnan, and A. Y. Halevy. Crowdsourcing systems on the world-wide web. *Commun. ACM*, 54(4):pp. 86–96, April 2011.
- [39] G Dólera Tormo, F Gómez Mármol, and G Martínez Pérez. On the application of trust and reputation management and user-centric techniques for identity management systems. *XII Spanish meeting on cryptology and information security (RECSI 2012), San Sebastián, Spain*, 2012.
- [40] P. Dumouchel. Trust as an action. *European journal of Sociology*, 46(03):pp. 417–428, 2005.
- [41] EDUCAUSE. Things you should know about... Federated Identity Management. Available online: <http://net.educause.edu/ir/library/pdf/EST0903.pdf>. Accessed: November, 2015.
- [42] T. El Maliki and J.M. Seigneur. A survey of user-centric identity management technologies. pages pp. 12–17, Oct 2007.



- 
- [43] D. Fraga, Z. Bankovic, and J.M. Moya. A Taxonomy of Trust and Reputation System Attacks. In *Proceedings of TrustCom 2012*, pages pp. 41–50.
- [44] K. K. Fullam, T. B. Klos, G. Muller, J. Sabater, A. Schlosser, Z. Topol, K. S. Barber, J. S. Rosenschein, L. Vercouter, and M. Voss. A specification of the agent reputation and trust (ART) testbed: experimentation and competition for trust in agent societies. In *Proceedings of AAMAS 2005*, pages pp. 512–518.
- [45] D. Gambetta. Can We Trust Trust? In Diego Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, chapter 13, pages pp. 213–237. 2000.
- [46] B. Gates. Bill Gates: Microsoft’s Security Vision and Strategy. *RSA 2006*.
- [47] E. Gianchandani. Darpa seeking to develop a cognitive fingerprint. *Computing Community Consortium Blog*.
- [48] D. Gollmann. Computer security. *John Wiley & Sons*, 1999. ISBN 0-471-97844-2.
- [49] N. Gomathy and D.N. Radha. A survey on single sign-on mechanisms for distributed computer networks. *International Journal of Computer Trends and Technology (IJCTT)*, 13(3):pp. 120–123, 2014.
- [50] The Open Group. Security forum on single sign-on. Available online: <http://www.opengroup.org/security/l2-sso.htm>. Accessed: November, 2015.
- [51] The Guardian. Amazon sues 1,000 ‘fake reviewers’. Available online: <http://www.theguardian.com/technology/2015/oct/18/amazon-sues-1000-fake-reviewers>. Accessed: October, 2015.
- [52] The Guardian. Are you suffering from password pressure? Available online: <http://www.theguardian.com/technology/2008/jan/17/security.banks>, 2008. Accessed: November, 2015.

- 
- [53] C. Haythornthwaite. Social networks and internet connectivity effects. *Information, Community & Society*, 8(2):pp. 125–147, 2005.
- [54] F. Hendrikx, K. Bubendorfer, and R. Chard. Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing*, 75:pp. 184–197, 2015.
- [55] C. Hillebrand and M. Coetzee. The design of a configurable reputation service. In *Trust, Privacy and Security in Digital Business*, pages pp. 60–70. Springer, 2015.
- [56] K. Hoffman, D. Zage, and C. Nita-Rotaru. A Survey of Attack and Defense Techniques for Reputation Systems. *ACM CSUR 2009*, 42(1):pp. 1–31.
- [57] J. Howe. The rise of crowdsourcing. *Wired Magazine*, 14(14):pp. 1–5, 2006.
- [58] Information Technology Security Evaluation Criteria (ITSEC). [https://www.bsi.bund.de/cae/servlet/contentblob/471346/publicationFile/30220/itsec-en\\_pdf.pdf](https://www.bsi.bund.de/cae/servlet/contentblob/471346/publicationFile/30220/itsec-en_pdf.pdf). Accessed: November, 2015.
- [59] J. Jensen. Federated identity management challenges. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, pages pp. 230–235, Aug 2012.
- [60] H. Jo, H. Jin Lee, K. Chun, and H. Park. Interoperability and anonymity for id management systems. *ICACT 2009*, 02:pp. 1257–1260.
- [61] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):pp. 618–644, 2007.
- [62] R. Jurca and B. Faltings. An incentive compatible reputation mechanism. In *Proceedings of AAMAS 2003*, pages pp. 1026–1027.
- [63] R. Kerr and R. Cohen. TREET: The trust and reputation experimentation and evaluation testbed. *Electronic Commerce Research*, 10(3-4):pp. 271–290, 2010.

- [64] M. Kinateder, E. Baschny, and K. Rothermel. Towards a Generic Trust Model - Comparison of Various Trust Update Algorithms. In *Proceedings of iTrust 2005*, number 2477, pages pp. 177–192.
- [65] A. Kobsa and J. Schreck. Privacy through pseudonymity in user-adaptive systems. *ACM Transaction on Internet Technology*, 3(2):pp. 149–183, May 2003.
- [66] O. Kussul, N. Kussul, and S. Skakun. Assessing security threat scenarios for utility-based reputation model in grids. *Computers & Security*, 34:pp. 1–15, 2013.
- [67] K. LaGrandeur. Cybersecurity and the Digitized Human. Available online: [https://www.academia.edu/15632553/Cybersecurity\\_and\\_the\\_Digitized\\_Human](https://www.academia.edu/15632553/Cybersecurity_and_the_Digitized_Human), 2015. Accessed: November, 2015.
- [68] J. D. Lewis and A. Weigert. Trust as a social reality. *Social forces*, 63(4):pp. 967–985, 1985.
- [69] S. Magin and S. Hauke. Towards engineering trust systems: Template-based, component-oriented assembly. In *Proceedings of PST 2013*, pages pp. 348–351.
- [70] T. Mahler and T. Olsen. Reputation systems and data protection law. *eAdoption and the Knowledge Economy: Issues, Applications, Case Studies*, pages pp. 180–187, 2004.
- [71] A. A. Malik, H. Anwar, and M. A. Shibli. Federated identity management (fim): Challenges and opportunities. In *2015 Conference on Information Assurance and Cyber Security (CIACS)*, pages pp. 75–82, Dec 2015.
- [72] F.G. Mármol and G.M. Pérez. Security threats scenarios in trust and reputation models for distributed systems. *Computers & Security*, 28(7):pp. 545–556, 2009.
- [73] F.G. Mármol and G.M. Pérez. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Computer Standards & Interfaces*, 32(4):pp. 185–196, 2010.

- 
- [74] F.G. Mármol and G.M. Pérez. Trust and reputation models comparison. *Internet Research*, 21(2):pp. 138–153, 2011.
- [75] S. P. Marsh. Formalising trust as a computational concept. 1994.
- [76] N. Miller, P. Resnick, and R. Zeckhauser. Eliciting honest feedback in electronic markets. In *Proceedings of SITE 2002*.
- [77] T. Miyata, P. Madsen, S. Adachi, Y. Tsuchiya, Y. Sakamoto, and K. Takahashi. A survey on identity management protocols and standards. *IEICE TRANSACTIONS on Information and Systems*, 89(1):pp. 112–123, 2006.
- [78] L. D Molm, N. Takahashi, and G. Peterson. Risk and trust in social exchange: An experimental test of a classical proposition. *American Journal of Sociology*, pages pp. 1396–1427, 2000.
- [79] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, and K. Klingenstein. Federated Security: The Shibboleth Approach. *EDUCAUSE Quarterly*, 27(4):pp. 12–17, 2004.
- [80] L. Mui. *Computational models of trust and reputation: Agents, evolutionary games, and social networks*. PhD thesis, Massachusetts Institute of Technology, 2002.
- [81] L. Mui, M. Mohtashemi, and A. Halberstadt. A Computational Model of Trust and Reputation for E-businesses. In *Proceedings of HICSS 2002-Vol.7*, pages pp. 188–.
- [82] S. K. Mukherjee and S. Neogy. Storage & retrieval of trusted information: A temporal probabilistic database approach. In *Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on*, pages pp. 1–15, Feb 2015.
- [83] B. C. Neuman and T. Ts'o. Kerberos: An authentication service for computer networks. *Communications Magazine, IEEE*, 32(9):pp. 33–38, 1994.
- [84] J. Pan, S. Paul, and R. Jain. A survey of the research on future internet architectures. *IEEE Communications Magazine*, 49(7):pp. 26–36, July 2011.

- [85] European Parliament. Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data. Available online: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>, 1995. Accessed: October, 2015.
- [86] S. Paul, J. Pan, and R. Jain. Architectures for the future networks and the next generation internet: A survey. *Computer Communications*, 34(1):pp. 2–42, 2011.
- [87] I. Pinyol and J. Sabater-Mir. Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, 40(1):pp. 1–25, 2013.
- [88] I. Pinyol, J. Sabater-Mir, P. Dellunde, and M. Paolucci. Reputation-based decisions for logic-based cognitive agents. In *Proceedings of AAMAS 2012*, volume 24, pages pp. 175–216.
- [89] E. Pournaras and S.J. Miah. From metaphor towards paradigm - a computing roadmap of digital ecosystems. *DEST '12*, pages pp. 1–6.
- [90] A. Princy and S. Vairachilai. A survey on single sign-on mechanism for multiple service authentications. *International Journal of Computer Science and Mobile Computing*, 2(12):pp. 40–44, 2013.
- [91] V. Radha and D. Hitha Reddy. A survey on single sign-on techniques. *Procedia Technology*, 4:pp. 134–139, 2012. 2nd International Conference on Computer, Communication, Control and Information Technology( C3IT-2012) on February 25 - 26, 2012.
- [92] K. S. Ramana and A. A. Chari. A survey on trust management for mobile ad hoc networks. *International journal of Network Security & Its Applications*, 2(2):pp. 75–85, 2010.
- [93] L. Rasmusson and S. Jansson. Simulated social control for secure internet commerce. In *Proceedings of the 1996 workshop on New security paradigms*, pages pp. 18–25. ACM, 1996.

- 
- [94] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. *Communications of the ACM*, 43(12):pp. 45–48, 2000.
- [95] P. Resnick and R. Zeckhauser. *Trust among strangers in internet transactions: Empirical analysis of eBay’s reputation system*, chapter 6, pages pp. 127–157.
- [96] J. Rotter. A new scale for the measurement of interpersonal trust. *Journal of personality*, 35(4):pp. 651–665, 1967.
- [97] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer. Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3):pp. 393–404, 1998.
- [98] S. Ruohomaa, L. Kutvonen, and E. Koutrouli. Reputation management survey. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, pages pp. 103–111. IEEE, April 2007.
- [99] J. Sabater and C. Sierra. Review on computational trust and reputation models. *Artificial Intelligence Review*, 24(1):pp. 33–60, 2005.
- [100] A. Sarma and J. Girao. Supporting trust and privacy with an identity-enabled architecture. *Future Internet*, 4(4):1016, 2012.
- [101] J.M. Seigneur. Trust, security and privacy in global computing. 2005.
- [102] S. Shenker. Fundamental design issues for the future internet. *IEEE Journal on Selected Areas in Communications*, 13(7):pp. 1176–1188, Sept 1995.
- [103] W. Sherchan, S. Nepal, and C. Paris. A Survey of Trust in Social Networks. *ACM Computer Survey 2013*, 45(4):pp. 47:1–47:33, 2013.
- [104] S. Singh and S. Bawa. A privacy, trust and policy based authorization framework for services in distributed environments. *International Journal of Computer Science*, 2(2):pp. 85–92, 2007.
- [105] T. J. Smedinghoff. Solving the legal challenges of trustworthy online identity. *Computer Law & Security Review*, 28(5):pp. 532–541, 2012.

- 
- [106] H. J. Smith, T. Dinev, and H. Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, 35(4):pp. 989–1016, 2011.
- [107] S. Srinivasan and R. Barker. Global analysis of security and trust perceptions in web design for e-commerce. *Int. J. of Inf. Security and Privacy*, 6(1):pp. 1–13, 2012.
- [108] S.T. Sun, K. Hawkey, and K. Beznosov. Openidemail enabled browser: Towards fixing the broken web single sign-on triangle. Aug 2010.
- [109] Y. Sun, Z. Han, and K.J.R. Liu. Defense of trust management vulnerabilities in distributed networks. *Communications Magazine, IEEE*, 46(2):pp. 112–119, 2008.
- [110] Y. Sun and Y. Liu. Security of online reputation systems: The evolution of attacks and defenses. *IEEE Signal Processing Magazine*, 29(2):pp. 87–97, 2012.
- [111] Y.L. Sun, Z. Han, W. Yu, and K.J.R. Liu. A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. In *INFOCOM*, pages pp. 1–13, 2006.
- [112] P. Sztompka. *Trust: A sociological theory*. Cambridge University Press, 1999.
- [113] The Telegraph. Users who post 'fake' Amazon reviews could end up in court. Available online: <http://www.telegraph.co.uk/news/shopping-and-consumer-news/11939070/Amazon-sues-more-than-1000-people-over-fake-reviews.html>. Accessed: October, 2015.
- [114] G. D. Tormo, F. G. Mármol, and G. M. Pérez. Towards the integration of reputation management in openid. *Computer Standards and Interfaces*, 2013.
- [115] G. D. Tormo, G. L. Millán, and G. M. Pérez. Definition of an advanced identity management infrastructure. *Int. Jour. of Infor. Security*, 12(3):pp. 173–200, 2012.

- 
- [116] J. Torres, M. Nogueira, and G. Pujolle. A survey on identity management for the future network. *IEEE Comm. Surveys and Tutorials*, 15(2):pp. 787–802, 2013.
- [117] T. R. Tylor. Why people obey the law. *Yale University Press, New Haven, CT*, 1990.
- [118] S. Vavilis, M. Petković, and N. Zannone. A reference model for reputation systems. *Decision Support Systems*, 61:pp. 147–154, 2014.
- [119] C.R. Vicente, D. Freni, C. Bettini, and Christian S. Jensen. Location-related privacy in geo-social networks. *Internet Computing, IEEE*, 15(3):pp. 20–27, May 2011.
- [120] M. Vinkovits and A. Zimmermann. TrustFraMM: Meta Description for Trust Frameworks. In *Proceedings of PASSAT 2012*, pages pp. 772–778.
- [121] M. Vinkovits and A. Zimmermann. *Defining a Trust Framework Design Process*, volume 8058 of *Lecture Notes in Computer Science*. 2013.
- [122] G. Wang, J. Yu, and Q. Xie. Security analysis of a single sign-on mechanism for distributed computer networks. *Industrial Informatics, IEEE Transactions on*, 9(1):pp. 294–302, Feb 2013.
- [123] J. L. Wayman. Biometrics in identity management systems. *IEEE Security Privacy*, 6(2):pp. 30–37, March 2008.
- [124] S. B. Wicker and D. E. Schrader. Privacy-aware design principles for information networks. *Proceedings of the IEEE*, 99(2):pp. 330–350, 2011.
- [125] Wikipedia. Federated identity. Available online: [http://en.wikipedia.org/wiki/Federated\\_identity](http://en.wikipedia.org/wiki/Federated_identity). Accessed: November, 2015.
- [126] Wikipedia. Password fatigue. Available online: [https://en.wikipedia.org/wiki/Password\\_fatigue](https://en.wikipedia.org/wiki/Password_fatigue). Accessed: November, 2015.



- 
- [127] C. Wu and E. Chang. Exploring a digital ecosystem conceptual model and its simulation prototype. In *Industrial Electronics, 2007. ISIE 2007. IEEE International Symposium on*, pages pp. 2933–2938. IEEE, 2007.
- [128] Z. Wu and A. C. Weaver. Requirements of federated trust management for service-oriented architectures. In *Proceedings of PST 2006*, page 10.
- [129] L. Xiong, L. Liu, and M. Ahamad. Countering feedback sparsity and manipulation in reputation systems. In *Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007. International Conference on*, pages pp. 203–212. IEEE, 2007.



# Acronyms

CMF	Content Management Framework
FCMF	Federated Content Management Framework
FIdM	Federated Identity Management system
FRMS	Federated Reputation Management System
IAE	Internet Alter Ego
ICR	Interaction Context/Role
IdM	Identity Management system
IdP	Identity Provider
MF	Main Features
MFV	Main Features Values
NoR	Number of Ratings
PII	Personally Identifiable Information
RMS	Reputation Management System
SAML	Security Assertion Markup Language
SOA	Service-Oriented Architecture
SP	Service Provider

SSO Single Sign-on

TEco Trust Ecosystem

TId Trusted digital Identity

TRM Trust and Reputation Management systems

TRR Trust, Reputation and Recommendation

TRR-MM Trust, Reputation and Recommendation Meta Model

# Index

## A

agreement, 22  
Agreement's Terms, 22

## B

Ballot stuffing, 42

## C

Content Management Framework, 25  
Context/Role Sliding, 42

## D

Denial of Service, 42  
Digital Identity, 19  
Direct Trust, 39  
Distrust, 37

## E

Ecosystem, 6  
Exit, 42

## F

Fake transaction, 41  
Federated Content Management Framework, 26  
Federated Identity Management, 19  
Federated Reputation Management, 21  
Feedback, 6

Future Internet, 18  
Future Network, 18

## H

Hard security, 13

## I

Identity Management System, 19  
Identity Providers, 10  
Indirect Trust, 39  
Inter Pares Interaction, 22  
Interaction Agreement, 22  
Interaction Context/Role, 22  
Interaction Token, 25  
Internet Agent, 22  
Internet Alter Ego, 19

## M

Main Features, 34  
Main Features Measurement, 34  
Main Features Values, 34  
Malicious Attacks, 41  
Meta IAE, 20

## N

negotiated agreement, 22  
Negotiated Interaction Agreement, 22

- 
- negotiation, 22  
Negotiation of the Agreement, 22
- O**  
Orchestrated, 42  
Oscillation, 42
- P**  
Password chaos, 10  
Password fatigue, 10  
PermIAE, 23  
Personally Identifiable Information, 12  
Promote, 41
- R**  
Reference RMS, 21  
RepTrap, 42  
Reputation, 38  
Reputation Management System, 21
- S**  
Self-promote, 42  
Single Sign-On, 9  
Slander, 41  
SOA, 31  
Soft security, 13  
Sybil Attacks, 41
- T**  
TempIAE, 23  
term, 22  
The right to be forgotten, 3  
Traitor, 41  
Trust, 37  
Trust Ecosystem, 6  
Trust, Reputation and Recommendation, 30  
Trust, Reputation and Recommendation Meta Model, 6  
Trust-Chain, 38  
Trusted digital Identity, 19  
TrustFraMM, 31
- U**  
UniTEC, 31
- W**  
Whitewash, 41  
Word of mouth, 38