An Open Distributed Identity and Trust Management Approach for Digital Community Ecosystems*

M.Ion, L.Telesca, F.Botto, H.Koshutanski
{mihaela.ion, luigi.telesca, francesco.botto}@create-net.org, Open distributed System for COmmunities (OSCO) Department, CREATE-NET (Italy)
hristo@lcc.uma.es, Computer Science Department, University of Malaga (Spain)

Abstract This paper explains how Community Networks (CNs), thanks to the Digital Ecosystem (DE) approach, can evolve towards Digital Community Ecosystems (DCEs) and proposes a model that would encourage the knowledge sharing and transactions between the members of different CNs. The model we propose allows CNs to rely on their offline world established business and trust relations to create better connectivity, collaboration and business opportunities between members of different CNs in the online world, functioning more like a DE. The model would encourage and enable SMEs to adopt web-based services reducing the necessity to register each time in order to be allowed access to a new ecosystem or service within an ecosystem. In particular, we focus on an easy to implement solution for bridging CNs trough a p2p system on top of which the identity and trust model can be deployed.

1 Introduction

Community Networks (CNs) can be understood as a hybrid community whose members meet online but share a geographic setting as well (Kavanaugh et al, 2005). There are many elements or dimensions involved in a CN (physical settings, community's features and members, technologies involved, and so on) and different kinds of CNs can emerge depending on the way in which these elements are mixed (Schuler, 1996; Chamtac et al, 2005). We define the major elements that are able to fully describe and characterize all the tensions involved in a CN are: Community, Infrastructures, Services, and Government (CISG Definition). Considering the relational and situated character of innovations (Star and Ruhleder, 1996), we can say that a CN is therefore when the tension between these dimensions gets to a point of balance. Each CN that has been developed combines those elements in a different way based on the community needs, the kind of services needed by the local community, the infrastructural needs or gaps, and last, but not least, the level of intervention of the public administration and the private sector. The mix of those elements reflects therefore a specific receipt that embeds the local tensions and that makes a CN implementation unique by definition. Therefore, CNs have been developed with the major intent to cover specific and localized needs without taking too much in consideration the potential synergies that these could have together beyond simple access to the internet. This lack of "interoperability" issue and joint development could be seen as the development of disconnected islands of knowledge that could provide problems in the further development of the local network. At the same time, within each CN, applications have been developed in different periods of time, independently from each other. Due to the lack of coordination and the early stage of interoperable software solutions, the synergies and economies of scale that CN

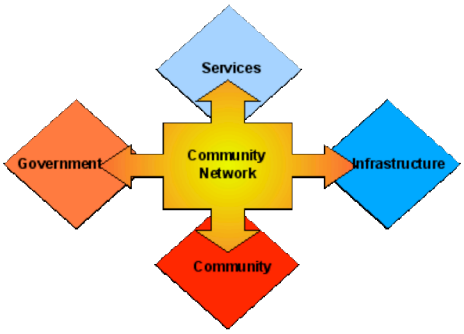

Figure 1: Community Network

* This work is partly supported by the projects: 038978 EU-MarieCurie-EIF-iAccess, 034744 EU-INFSO-IST ONE and 034824 EU-INFSO-IST OPAALS.

could have pursued at software level with a more Service Oriented Approach (SOA[1]) have not been pursued.

A Digital Ecosystem (DE) represents a step towards this direction. DE is a pervasive and open digital (software) environment in which organizations and individuals interact to share knowledge, develop and share services and offer goods of value to users, who are themselves members of the ecosystem (Dini, 2007). A DE therefore includes all community stakeholders. The relations between the members of a DE are complex and dynamic and evolve in time. As opposed to CNs, DEs take for granted the existence of a broadband infrastructure that connects members (SMEs, users, others) to the DE. Online business interactions are therefore mainly constrained by connectivity issues. As opposed to DE, in CNs business relations are more difficult to create due to identity and accountability issues caused by the lack of interoperability of the applications. Online business interactions are therefore mainly based on the offline world relations between organizations and individuals.

2 The Digital Community Ecosystem Model

The DE concept has been created by referring to the business world. It grew up in recent years in order to be help considering the digitalization of Business Ecosystems (Moore, 1997). Although DEs cover a more business oriented vision while CNs deal more with the non-for-business world, they both have a strong connection to e-participation and social responsibility issues. Thanks to DEs and their interoperable software approach, CNs could scale to more open systems becoming interoperable both at local and global level. DEs can leverage on the open infrastructure developed in the CNs as a gateway to local communities, local knowledge and services. Therefore we introduce here the concept of Digital Community Ecosystem (DCE). DCE is an open access infrastructure and software environment that provides the possibility to develop, share, sell and deploy interoperable services that enhance computer mediated communication at local and global level. Each CN could deploy and use a DE approach to develop an interoperable local DCE where interoperable services could be deployed and could also easily connect to other DCEs. One of the main conditions to make this happen is to develop an identity and trust model that is able to cope with the before mentioned approach. In the work (Telesca & Koshutanski 2007), the authors propose a new multidisciplinary approach for evolutionary trust. The authors propose a framework that bridges security models for trust with reputation and learning in order to form a coherent evolutionary trust model for DEs. In order to provide inter-ecosystem interoperability, an identity management model (Koshutanski, Ion & Telesca 2007) suitable for the dynamic nature of DCEs has been developed.

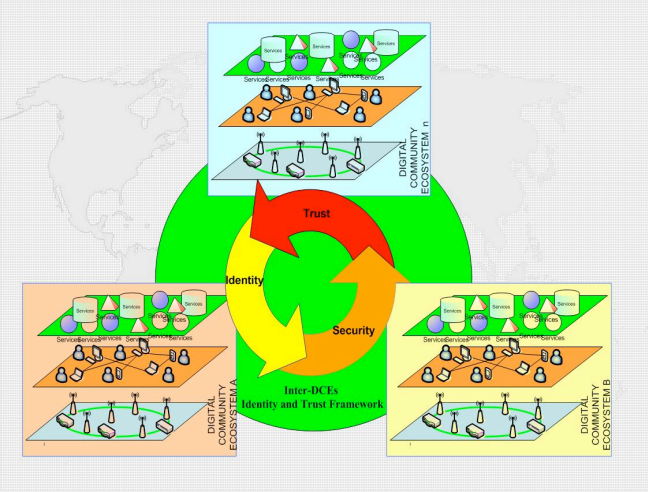

Figure 1. The Distributed Identity and Trust Management Model for DCEs

The DCE concept could be beneficial for all the regions, especially developing ones, where information infrastructure investments are still missing or underdeveloped.

[1] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm

Using from the beginning this innovative approach, local stakeholders could develop a sustainable and interoperable environment that could drive local development. Innovators could benefit both in term of cost reductions for a new service set-up and in term of new business opportunities for local business players.

3 The Distributed Identity and Trust Management Model for DCEs

To allow DCEs to interact online, we propose a peer-to-peer network for interconnecting the different actors involved in DCEs. This kind of infrastructure fits the DCE because it is easy to install and maintain, it is decentralized, and allows actors to interact directly and leave and join the system when they wish without affecting the stability of the platform. On top of the peer-to-peer network, a distributed identity management system which enables interoperability between different organizations provides the basis for building social responsibility through trust and accountability.

3.1 Identity Management

This section outlines the main features of the identity management model (Koshutanski, Ion & Telesca 2007) suitable for the dynamic nature of DCEs.

Managing identities in a DCE poses many challenges. First of all, institutions use different types of certificates and identity technologies (e.g. X.509, SPKI and Kerberos) which are not always compatible with each other. Secondly, users often need to access applications, services or a composition of services located on different administrative domains. Finally, because of the dynamic nature of the environment, federating and sharing of identities becomes a complex task. A pure federating approach is viable only when there is a stable relation. In DCEs, federation does not scale up because of the unstable and ad-hoc coalitions.

Our model focuses on providing ways for exchanging identity information between companies independent of the standards they use and on sharing user identity between different domains which could be federated or have no direct trust. WS-Policy[2], WS-Trust[3] and WS-Federation[4] cover a wide range of requirements, but are difficult to suit immediately for small and medium size enterprises (SMEs). We propose a targeted model that is easy to understand and straightforward to implement and put in practice. We accommodate all kinds of users: companies and users which may own a computer or not. We provide simplicity for users: users login using username & password and the handling of certificates and identification is done automatically by the system through the use of user profiles stored in the network. A user profile is an abstract view of a client's identity information and is stored in a decentralized manner, on trusted peers.

The model is based on the new SAML[5] (v2.0) standard for providing proper identification. SAML provides interoperability on the message level and helps to automate and converge when the technologies are not compatible.

All users are considered equal and there is no hierarchy of DCEs. Any peer can be a Credential Provider (CP) or a Service Provider (SP), or both. Each user (who has the capability) can issue a certificate to other users. Each user has a list of trusted CP. Each CP has a list of accepted security tokens.

The user is only required to remember a username and password in order to login into a DCE. The username and password are created when the user initially registers to a DCE. Then, whenever the user logs in another (or the same) DCE by presenting its username and password (just authentication), the DCE takes the responsibility to allocate

---

[2] http://www.ibm.com/developerworks/library/specification/ws-polfram/

[3] http://www.ibm.com/developerworks/library/specification/ws-trust/

[4] http://www.ibm.com/developerworks/webservices/library/ws-fed

[5] OASIS Security Assertion Markup Language: http://www.oasis-open.org/committees/security

and retrieve the encrypted user profile. Each DCE has its predefined trusted node(s) which stores information on DCE users and addresses trusted nodes residing in other DCEs. At the end of business, the user's profile is encrypted and updated on the associated trusted node (peer) and then replicated on the other trusted peers.

More details on the model can be found in (Koshutanski, Ion & Telesca 2007). Below we describe the basic identity model and workflow of messages between the model's components. Figure 2 shows the model and the steps behind the model: (1). An entity (web browser user or local client) makes a request to a SP. (2-3). The SP redirects the user to a Trusted Credential Provider (TCP). (4). The user has no credentials issued by the TCP. The TCP sends a list of accepted certificates with a list of its trusted CPs to the user. (5). The user requests its profile from a trusted peer storing it and uses username/password for authentication. Information for ecosystem trusted peers is obtained (possibly publicly available) when users join the ecosystem. (6). The trusted peer sends the encrypted user profile. (7). After the profile is decrypted, the user checks if it has the right credentials, i.e. processes his profile for matching of credentials (issued by any of the TCPs obtained in step (4). If no credential is matched, the user has to register to the TCP to obtain an identity token. If one of the credentials requested in step (4) is found, then the user extracts it either from the profile or requests it from the remote TCP that issued it.

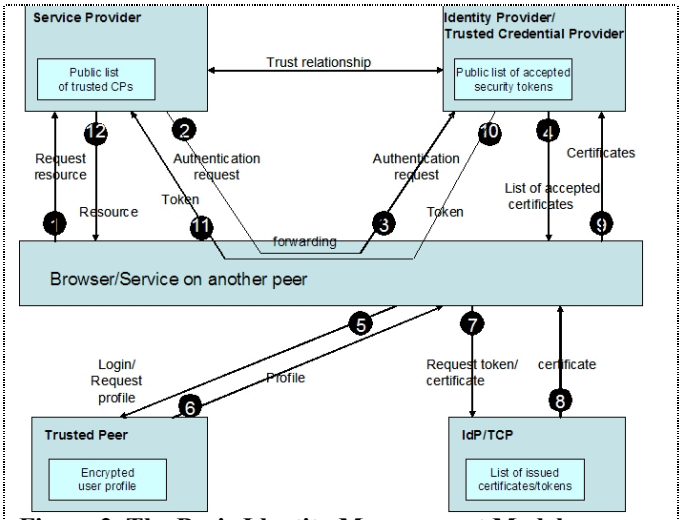

Figure 2. The Basic Identity Management Model

(8). The TCP authenticates the user and then returns either the requested certificate or its transformation to a SAML assertion. (9). The user forwards the certificate/SAML assertion to the TCP. (10). The TCP verifies and validates the certificate and issues (transforms if needed) a new one that is to be forwarded to the SP. (11). The user is redirected to the Service Provider which accepts tokens from its TCP. (12). The Service Provider verifies the new certificate and provides the requested resource to the user.

DCEs allow companies to cooperate with each other and compose services. An important requirement for an identity management model for DCEs is to support composition of services. The basic model can be extended to cope with the case in which one service relies on services from other cooperating partners. In a service composition scenario, the SP aggregating services from other SPs needs to run the services on the name of the user and to do so, he has to authenticate the user to the other providers. To solve this problem we adopt the use of Proxy Certificate[6] that the client issues to the provider of the composite service.

3.2 Trust Management

The trust model built on top of the identity management system is based on institutional trust created in the offline world, and on trust relationships and history of experiences from the online world. Individuals and institutions which already have a trust relation in the offline world can connect and assign high trust values and issue certificates to each other in the online world. In this way, users create a network of trust on top of the peer-

[6] Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile: www.ietf.org/rfc/rfc3820.txt.

to-peer system. Users are then free to further interact with unknown peers in the system and ask the opinions of others before they transact. Based on transactions outcome, peers assign ratings to other peers. By aggregating these scores, a reputation value can be computed for each peer. By transacting in the online world, the pre-established relations between peers evolve and new ones are created. Moreover, several levels of trust can be created involving different aspects of the interactions (e.g. users, institutions, infrastructure, CNs, data). The trust model is based on two components: peer to peer reputation system and distributed rating agencies.

3.2.1 Peer-to-peer Reputation System

A peer to peer reputation system allows peers to cooperate with each other in order to assign reputation values to all peers in the system. A reputation system is a purely distributed approach in which reputation values are stored and computed among peers without the intervention of a big-brother.

In our model, every user keeps a history of peers and actions/events performed with other peers quantified with average trust score together with information about the number of transactions, the time at which the most recent transactions occurred and the value of the transactions. If a user is known from the offline world, the user will receive a trust value when first joins the system based on the pre-existing relation. Users who belong to a company already known in the system are attached a trust value derived from that of the company taking into consideration the position inside the company.

In our p2p reputation model, each user has a history H of events and actions performed with other peers and a level of satisfaction with each of them. When a decision based on peer reputation needs to be made, the agent computes using its reputation model *M* and history *H* a level of trust to place in a peer and decides whether to transact or not.

In this way, each reputation model M is dynamic and can evolve in time. Based on a growing history H, a model M can learn new reputation rules. Reputation rules reflect what an agent's trust behavior is and how from existing reputation values and events, *new* events and behavior can be derived. When a new event or behavior is derived, it is automatically added in the history *H* so that in future steps an agent can derive new recommendation values based on his derived knowledge in the past. Thus the agent's behavior can self-adapt and evolve over time.

After every transaction, the reputation information is updated. In computing the trust value, the most recent transactions count more and the value of transactions in taken into consideration. A defection on a $100 transaction weighs more then one on a $1 transaction.

Transaction feedback is made available to all users of the system. The ratings of each peer will be stored by several peers in the system. Providing transaction feedback is voluntary. When a user wants to provide feedback about a peer, it uses several hash functions to determine the peers which store the trust information of the rated peer. Every user is autonomous and can either rely on the overall value computed by the system or compute the reputation value separately, by a preferred algorithm. This approach accommodates both simple users who do not have a computer and enterprises that benefit from an IT infrastructure.

3.2.2 Distributed Trusted Rating Agencies

Rating Agencies are traditionally a centralized solution in which a trusted authority gathers ratings from different actors, computes a global value or ranking for each actor, and issues certificates including this rating to registered users. Having one such agency would not accommodate the distributed nature of DCEs. We propose an approach similar with the identity management model described above. Each community in the DCE will have one or several rating agencies and the agencies will cooperate with each other to

translate certificates issued by an agency not known to the community. The translation involves two aspects: interoperability between different rating schemes and representations, and a trust relationship between different agencies.

The reputation scores will be computed based on a criteria similar to the one used for the p2p reputation system. However, the rating agencies can use a more complex algorithm and store historical data which can be used for deriving patterns. Agencies store user profiles created when the user registers with them. A learning component can be used to predict user behavior based on profile and past behavior.

4 Conclusions and Future Work

The trust model together with the identity management system we presented in this paper enables building accountability and social responsibility in the DCEs. This approach offers a secure environment in which entities in DCEs can establish safe business relations and make profitable online transactions. The model will not vary from developing nations to developed world but will be easier to adopt in emerging markets rather then in developed ones since it is easy to deploy and does not require expensive infrastructure and software investments. In the next future we will analyze and assess the scalability and effectiveness of the identity and p2p reputation model through simulation. Later on we will also validate our model during real life tests in different business scenarios.

References

Chlamtac I., Gumaste A. and Szabo C. A. (Eds. 2005) Broadband Services: Business Models and Technologies for Community Networks, Wiley, Chichester.

Dini P. (2007) "A scientific Foundation for Digital Ecosystem", to appear

Kavanaugh A., Carroll J.M., Rosson M.B., Zin T.T. and Reese D.D. (2005), "Community Networks: Where Offline Communities Meet Online"; in Journal of Computer Mediated Communication, 10(4), article 3. http://jcmc.indiana.edu/vol10/issue4/kavanaugh.html

Koshutanski H., Ion M., and Telesca L. (2007) Distributed Identity Management Model for Digital Ecosystems. In Proceedings of International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'07), (October), Valencia, Spain, IEEE press.

Moore L. (1997) Death of Competition: Leadership and Strategy in the Age of Business; HarperCollind Publishers, New York.

Schuler D. (1996) New Community Networks: Wired for Change. Reading, MA: Addison-Wesley. http://www.scn.org/civic/ncn

Star S.L. and Ruhleder K. (1996) "Steps Toward an Ecology of Infrastructures: Design and Access for Large Information Spaces"; in Information Systems Research, 7(1):111-134

Telesca L. and Koshutanski H. (2007) A Trusted Negotiation Environment for Digital Ecosystems. In F. Nachira, M. Le Louarn, L. Rivera Lèon (eds) Building the foundations of Digital Ecosystems: FP6 Results and Perspectives. Publisher: European Commission.