International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.171-184
http://dx.doi.org/10.14257/ijsia.2016.10.2.16

On the Deployment of Citizens' Privacy Preserving Collective Intelligent eBusiness Models in Smart Cities

Artemis Avgerou[4], Panayotis E. Nastou[1,3*], Dimitra Nastouli[4], Panos M. Pardalos[1,2] and Yannis C. Stamatiou[4,5]

[1]*Center for Applied Optimization, University of Florida, Gainesville, USA*
[2] *Department of Industrial Engineering and Systems, University of Florida, Gainesville, USA*
[3]*Department of Mathematics, University of Aegean, Samos, Greece*
[4]*Department of Business Administration, University of Patras, Patra, Greece*
[5]*Computer Technology Institute and Press ("Diophantus"), Patra, 26504, Greece*
[1,2]*pardalos@ise.ufl.edu,* [3]*pnastou@aegean.gr,* [4]*artemisavg@gmail.com, nastouli@upatras.gr,* [5]*stamatiu@ceid.upatras.gr*

Abstract

During the last two decades the world is being transformed towards a virtual agglomerate of large interconnected cities. Moreover, an integration of digital infrastructures with the physical city infrastructure and facilities is taking place. This integration includes data generating sensors and various internet-connected devices which are dispersed in a city having as a target to offer a variety of services in order to ease citizens' daily lives. In this, so called, smart city digital ecosystem, companies provide eBusiness models that are based on Collective Intelligence based decision making applications focusing on discovering citizens' needs by collecting data related to their activities. However, the lack of privacy preserving mechanisms in such applications that eliminate the risk of correlation between citizens' activities and their identities discourages citizens from providing their data to commerce systems. In this paper, we first discuss a new privacy preserving authentication technology, the Privacy-ABCs, and its successful deployment in a course evaluation pilot in higher education as well as a social networking application for pupils in a school environment. Based on the wide acceptance of this technology by the pilot users, we propose the deployment of a Privacy-ABCs based authentication system in a generic Collective Intelligent eBusiness model in a Smart City. The incorporation of this authentication technology in Collective Intelligence based eServices, has the potential of establishing new market opportunities since citizens' anonymity will increase their incentives to provide valuable data related to their consuming activities and buying preferences as they move about in the city.

Keywords: *Smart Cities; Privacy; Collective Intelligence; eBusiness Models; eServices*

1. Introduction

Nowadays, the majority of world's population lives in big cities. It can, also, be said that the earth's population resides in a world of interconnected cities. A contemporary city attempts to improve the quality of citizens' life (better transportation, energy consumption, e-governance etc.) and its economy by integrating digital infrastructures with the physical facilities of the city ([1, 5]). This integration can make a city "smarter" in the sense that a city can learn about

*Panayotis E. Nastou is the Corresponding Author
This paper is a revised and expanded version of a paper entitled " Adopting an ABCs Authentication Framework for Collective Intelligent eBusiness Models in Smart Cities" which will appear in the Proceedings of the 8th International Conference on Security Technology, Jeju Island, Korea, November 25-28, 2015

ISSN: 1738-9976 IJSIA

citizens' needs and to provide services that improves its citizens' life anytime and in any place around the city.

Within the current decade, many ICT vendors invested on products that can transform a city into a *smart city*. Companies from the public and private sector develop or use crowd-sourcing applications that collect and analyze massive data related to the environment and citizens' way of life (data from home smart meters, electricity operators' systems, citizens through their interactions using smart phones, public information systems, social network applications and other corporate data sources). These applications are based on the Collective Intelligence (CI) which is the intelligence that emerges from the participation of many individuals and/or devices of a group in a consensus decision-making context. The use of CI in business exploits the mass collaboration in order to create new markets for goods and consequently new industries and jobs and to reduce operational costs.

Mobile network operators have a central role in the smart city concept. They provide the medium through which citizens offer useful data in order to receive smart services. Thus, CI-based consensus decision making systems would aggregate large data streams from various network devices through mobile networks and other internet connected data sources and would create services for the citizens and the city. The data aggregation and smart service deployment are taking place through internet.

However, this society evolution and the new come out business models in a smart city, i.e. the design of organizational structures that create new commercial markets and products for citizens, should be associated with system architectures that can support them efficiently [1]. This system architecture evolution could happen in a similar way that mobile networks and business models affected by the introduction of smart individuals' devices. Smart city business models could demand a large amount of devices to be connected either to mobile networks or to fixed networks. Consequently, data aggregation by CI-based applications of the related business models will induce bulky load on the networks.

Humans are playing the central role in the majority of the business models that are based on CI-based decision making applications. Actually citizens are working for free while they are offered free services. Smart city applications should consider citizens' data as a public good for civil improvement (see in [1]) but their privacy should be preserved. Not only should the legislation protect their privacy but the smart city applications should use Privacy Enhancing Techniques (PETs) for their privacy (see in [2]).

Smart Location Based Services that provide to mobile users information for certain requests, like the closest gas station and parking place for example, collect the physical location of a user. Moreover, other services can collect data from various city storages where a user may have left her footprints. However, some city services demand from the user to provide her identity in order to access the service. All these user related data could be used to correlate users with their activities. These users' profiles would be valuable for the creation of target groups for certain new e-Services. Thus, there is a need in the concept of a smart city to protect citizens' privacy. Protecting citizens' privacy will increase citizens' incentives to participate in the creation of new markets and services through CI-based business models. This could be achieved by eliminating the potential correlation of a user with her activities that discourage her to provide data. The design of an identity management system that would permit the collection of citizens' data that are sufficient according to the principle of data proportionality, i.e. the minimum subset of identity data, for the accomplishment of the purpose of the citizens' data collection can eliminate this correlation without affecting the trust between citizens and the companies that collect data and provide services.

Identity management consists of all these processes and underlying technologies that create, manage and use digital identities (see in [7]). The need of individuals and businesses to verify whether a presented identifier or identity is actually representing the entity one trusts or that is entitled to enter into a certain transaction or communication was the initiative for the design and development of access control and personal data management techniques that will protect individuals' privacy. Users prove their identity through various authentication mechanisms. One widely used authentication mechanism is the password-based authentication. Today, individuals are asked to maintain dozens of different usernames and passwords, one for each website with which they interact. This authentication mechanism is not always optimal, since it creates a burden to individuals and encourages the reuse of passwords through multiple services, which in turns makes online fraud and identity theft easier. Spoofed website, stolen passwords and compromised accounts have negative impact not only to individuals but also to businesses and governments, who are unable to offer high-value online services.

Given the weaknesses of such a simple authentication mechanism, alternative techniques have been developed to provide a higher degree of access control and personal data management. Cryptographic certificates are a good known example of this. Although such certificates can offer sufficient security for many purposes, they cannot, typically, handle privacy adequately because they reveal completely the identity of a person. Any use of such a certificate exposes the identity of the certificate holder to the party (usually a service) requesting authentication. There are many scenarios where the use of such certificates reveals, unnecessarily, the identity of the holder. For example, this is the case for scenarios where a service platform only needs to verify the age of a user but not his/her actual identity. Revealing more information than necessary not only harms the privacy of the users but also increases the risk of abuse of information such as identity theft when revealed information falls in the wrong hands.

In this paper, we present the deployment of a Privacy-ABCs based authentication system into a generic eBusiness model that provides Collective Intelligence based eServices in Smart Cities. These Collective Intelligence eServices can establish new market opportunities in which citizens' anonymity will increase their incentive to provide valuable data about their consumer behaviour. In Section 2, we discuss the use of Privacy-ABCs, which is an attribute based authentication technology, in course evaluations in higher education and social networking for pupils in a school environment. In Section 3, we discuss the structure of a deployment of an ABCs based authentication system in a generic Collective Intelligence eBusiness model in a smart city. Finally, in Section 4 we present our conclusions and discuss directions for future work.

2. Attribute-Based Authentication

A number of technologies have been developed to build Attribute Based Credential (ABC) systems in a way that they can be trusted, much like normal cryptographic certificates, while at the same time protecting the privacy of their holder (e.g., hiding the real holder's identity). Such certificates, called Attribute Based Credentials (ABCs) are issued just like ordinary credentials using a digital (secret) signature key. However, ABCs allow their holder to transform them into a new credential that contains only a subset of the attributes contained in the original credential. Additionally, these transformed credentials can be verified like ordinary cryptographic credentials (using the public verification key of the issuer) and offer the same strong security.

Two prominent technologies are IBM's Idemix, based on [4, 12, 13, 14, 15] and Microsoft's Uprove, based on [6, 10] (see, also in [3, 11] for preliminary research work). In the ABC4Trust project (http://abc4trust.eu), an integration in a seamless and interoperable way of these two technologies into a single one called *Privacy-ABCs* were proposed. In any deployment of Privacy-ABCs (see Section 3 for more details), first credentials need to be obtained from the Credential Issuer with an issuance request and the User provides the appropriate credentials. These steps need to be performed only once. Collected credentials are stored and managed on the User side, under her total control. Consequently the Issuer may well be offline or unreachable for one or both parties, the User and the Verifier (or Relying Party), during subsequent authentication processes. Specifically, whenever the User wishes to access a restricted resource offered by a Verifier, she will request access to this resource. The Verifier answers by providing the access policy for the requested resource. Such a policy might refer to requirements with respect to any user attribute, e.g. the user's name, being of a certain age, or being a member of a university.

The client module on User's side helps the User computing a presentation token satisfying the access policy. This step may include the removal of any personal data not required by the policy. The resulting presentation token is then presented towards the Verifier for cryptographic verification of the possession (without revealing them) of the claimed attribute values. The ABC4Trust project's strength was the operation of two pilot, but real life, applications in the educational domain. The pilots involved real users with real use cases and, thus, enabled the project participants to draw useful conclusions about the easiness of implementing Privacy-ABCs solutions and how well they are accepted by users. In what follows, we will provide some essential information on these two pilots which are related to this work.

Protecting the privacy of children in a school environment involved pseudonymous community access and social networking for pupils in Sweden. This pilot handled online communication and exchange of sensitive personal concerns and advice between pupils and school personnel. Pupils were able to seek advice from medical staff or teachers on intimate questions related to their physical, psychological, social, financial, or other situation without necessarily revealing their true identity. They were, also, able to communicate among themselves in special restricted areas where access can be granted only to students of, e.g., a certain age or sex. This part of the pilot exploited the advantages of the ABC technology by allowing anonymous proofs of attribute values.

Course evaluations in higher education was the second pilot of the project. It involved the issuance of privacy preserving credentials to the students of the University of Patras in Greece, that certified a number of facts about the students (e.g. year of study, major, percentage of appearances in the lecture room in case of obligatory courses, etc.). Eligible students were able to provide feedback *anonymously* on the courses they had taken as well as their instructors during a semester, proving their eligibility using the appropriate credentials.

Our project took the pilots one step further and evaluated participating users' attitude towards ABCs as well as their willingness to adopt and use this privacy preserving authentication technology. Our view is that this technology has the potential of changing the way people think about and interact with ICTs and the Internet services, such as the one envisages in our eBusiness model. ABCs, through their privacy preserving features, can transform the online society into a more trustworthy one and allow the development of online businesses and services of wide adoption from the people. For this to happen, however, it is not sufficient to base the online world on excellent, technically, privacy and security technologies.

One needs to, also, ensure that these technologies will attract the major stakeholder, that is the users.

The ABC4Trust project not only provided the reference implementation of the ABCs technology making it publicly available to developers of eServices, it did conduct a systematic user experience evaluation from the pilot participants as well. Through thus evaluation, the ABC4Trust project attempted to tackle the following questions, which are directly relevant to our proposal to use the ABCs technology in new territories, beyond education (which was the focus of the two ABC4Trust pilots) such as eBusinesses and general eServices:

- What are the factors (both internal to the user and external) and parameters that influence user acceptance of ABCs?
- What are the key factors that enable users to view ABCs as a trustworthy technology and the services built on top of it as trusted?
- How good is users' understanding of ABCs and what is the role of this understanding in enhancing users' acceptance?
- How one can transform users' evaluation results into improvements of ABCs and the services that can be build using this technology?

Both pilot leaders investigated users' acceptance using the *Technology Acceptance Model (TAM)*, a very successful predictive model for assessing user acceptance of ICTs (see in [16, 18]).

TAM was developed in the 80s [17] and has been employed for the evaluation of a wide variety of technological products (e.g. from email and spreadsheet software to online games). The general framework of the Technology Acceptance Model [16, 18]. The overall TAM framework is depicted in Figure 1.

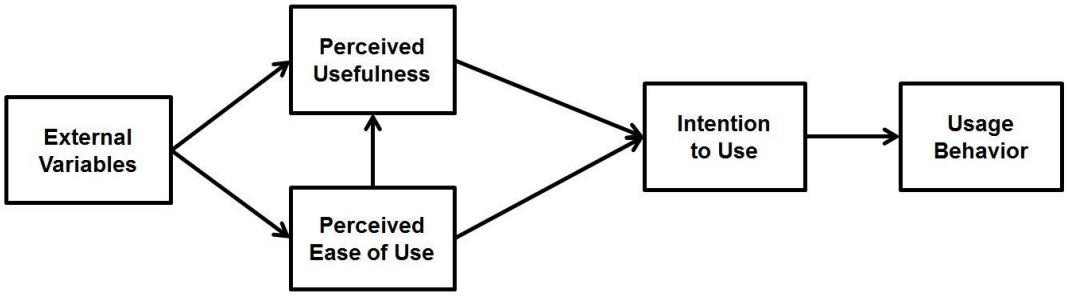

Figure 1. The General TAM (Technology Acceptance Model) Framework

TAM regards the *Perceived Ease of Use* and *Perceived Usefulness* of a new technology as the two main factors that decide users' adoption of the technology [16, 17]. Positive attitude of users towards these two factors positively influences their *Intention to Use* the new technology which, in turn, positively influences their actual *Usage Behavior*. Moreover, *Perceived Ease of Use* influences *Perceived Usefulness*, in the sense that Perceived Usefulness is considered to have a more powerful direct influence on the widespread adoption of the new technology than Perceived Ease of use.

The TAM factors are defined as follows:

- *Perceived Ease of Use*: "the degree to which a person believes that using a particular system would be free of effort".
- *Perceived Usefulness*: "the degree to which a person believes that using a particular system would enhance his or her job performance".
- *Intention to Use*: "the degree to which a person has formulated conscious plans" to use or not to use a specific technology".

- *Usage Behavior*: "the actually observed and measured usage", e.g., frequency and duration of the usage.

The TAM framework, also, includes external factors that may exert influence on Perceived Usefulness and Perceived Ease of Use [18, 19]. Such factors include characteristics of the new technology or system (e.g., relevance of the system to work or expertise, perceived quality of system's results and outputs), differences between the user' characteristics and idiosyncrasies (e.g., age, sex, job experience, specialty, knowledge of ICTs etc.) or, even, characteristics of the users' environment (e.g., technical and managerial support when needed, influence from other users etc.).

By taking into account the collection of criteria and the implementation of necessary infrastructure (identity service provider, infrastructure to issue credentials, attribute databases, etc.), the evaluation of these pilots with the TAM framework provided a clear proof of concept of both the unified attribute-based credentials approach as well as the reference architecture, providing at the same time feedback for enhancement.

The pilots were successful in providing a strong proof of concept of the applicability of Privacy-ABCs in real life applications. The evaluations provided by the users who participated in the pilots showed satisfaction, to a large degree, as well as easiness of use and deployment (see [8, 9]) for more details on the formal user satisfaction survey we conducted within the context of the ABC4Trust project for the course evaluation pilot – similar results have been documented for the school pilot in the corresponding project deliverable).

3. Incorporating Privacy-ABCs Framework into CI eBusiness Models

The deployment of eServices that respect users' privacy, requires the existence of a *Trusted Third Party (TTP)*. Both the user and the eService provider will develop mutual trust through a TTP. The Privacy-ABCs technology provides an entity, the Issuer, which can play the role of TTP entity in an eBusiness Model. In Figure 2, the entities and their interactions in a Privacy-ABCs based eBusiness Model are illustrated. The user is in the center of this eBusiness Model.

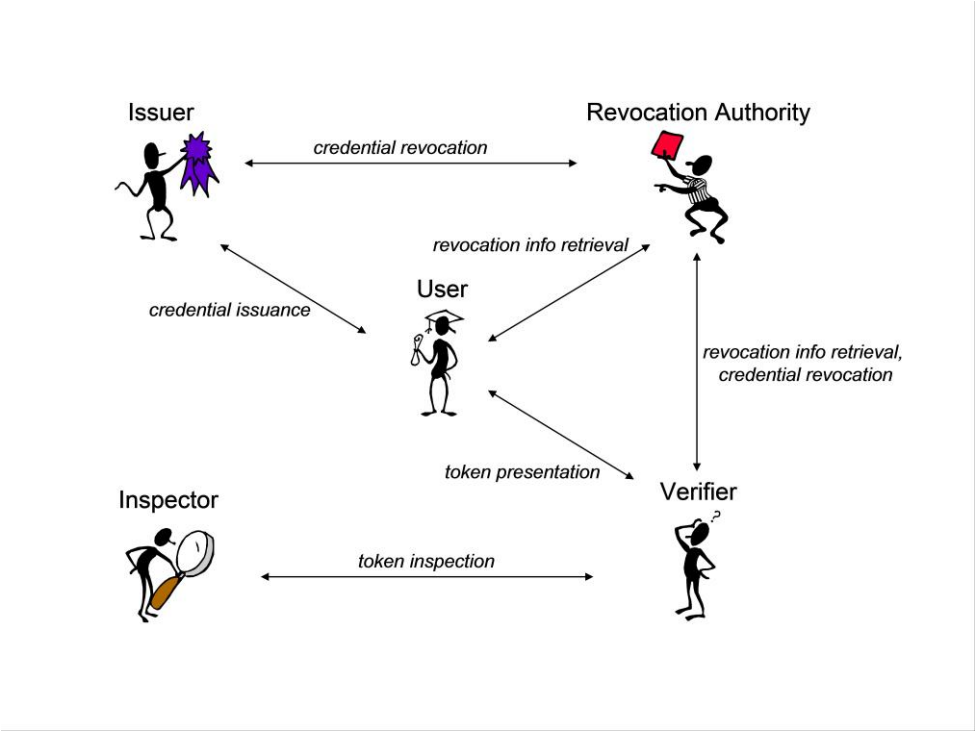

Figure 2. The Entities and their Interactions in a Privacy-ABCs eBusiness Model

The Issuer generates credentials containing attributes and provides them to the User who requested the issuance of the credentials. A credential is a set of attributes issued, and certified, by the Issuer. An attribute consists of the attribute type that describes the semantics of the attribute (e.g. first name) and the attribute value that determines its contents (e.g. Artemis). The Issuer certifies the correctness of the attributes that the credential contains. These attributes are identity elements and information about the User. A *credential specification* defines a list of attribute types that are contained in a credential. Initially, the Issuer creates a set of parameters, the *issuer parameters*, and a secret key, the *issuance key*. The credential specification and the issuer parameters will be used by the verifier in order to verify the authenticity of the user‘s presentation token which is created from the issued credential. The issuance key is used by the issuer in order to issue credentials.

Depending on the use case, the attribute values of a credential may be provided either by the User or the Issuer, if the Issuer already holds the respective information in its attribute database. Ideally, the Issuer can provide the attested information directly, being an authoritative source. In a smart city, the Issuer can be a public service which will be under the control of the municipality. This guarantees that the citizens’ rights will be protected by the legislation.

The Issuance of a credential is an interactive multi-round protocol between a user and an issuer. It is initiated by the user by sending a message request for a credential (see in Figure 3). The issuer initiates an authentication process of the user. Upon its completion, it sends a message that contains the set of attributes that shall be certified in the new credential, the issuer policy and the issuer parameters of the credential. The user and issuer exchanges a number of protocol messages and at the end of the protocol, the user’s system stores the obtained credential for future use.

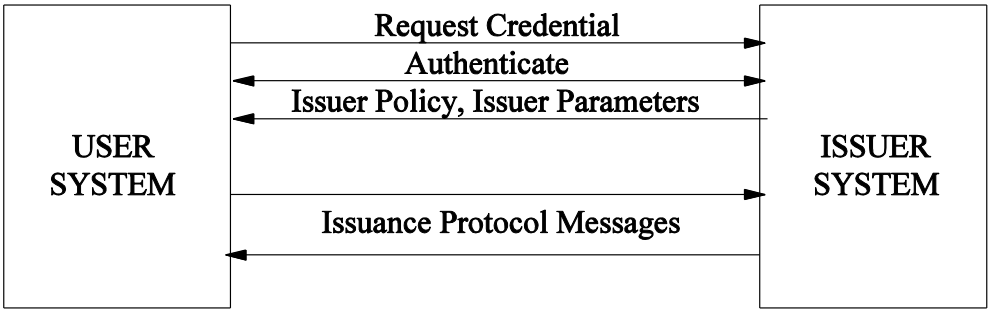

Figure 3. The Multi-Round Privacy-ABC Issuance Protocol

An optional entity of a Privacy-ABCs authentication system is the Revocation Authority that is responsible for revoking issued credentials. After revocation, the credentials cannot produce valid presentation tokens (i.e. proofs about credentials). In our smart city eBusiness model, the entity offering the revocation service is the same as that offering the Issuer service, which can be assumed to have the most accurate information about users' attributes and credentials.

Each user generates a secret key which is used to generate public keys. These public keys are called *pseudonyms* in Privacy-ABCs. A user deploys pseudonyms for accessing services anonymously. Unlike traditional public-key authentication schemes, however, there are multiple public keys corresponding to the generated secret key. Consequently, the user can generate as many public keys as she wishes. Pseudonyms are cryptographically unlinkable, meaning that given two different pseudonyms, one cannot tell whether they were generated from the same or from different secret keys. By generating different pseudonyms for different verifiers (i.e. service providers), users can be known under different unlinkable pseudonyms to different sites while using the same secret key to authenticate herself towards all of them. While it is sufficient for users to generate a single secret key, they can also have multiple secret keys. A secret key can be generated by trusted hardware (e.g., a smart card) that stores and uses the key in computations (e.g., to generate pseudonyms) while never revealing it. The key is thereby bound to the hardware, in the sense that it can only be used in combination with the hardware.

An eBusiness Model that would provide CI Services should encapsulate in its structure the Verifier which is the basic entity of a Privacy-ABC authentication framework. The Verifier usually provides some kind of access restricted service to the User to which the User needs to authenticate and imposes an access policy. Thus, a User that intends to access a restricted service, the provider of the service launches its Verifier entity to authenticate the user. The authentication process is based on a presentation token provided by the User allowing it to check that the User has certain attributes. Upon the reception of the access request by the User, the Verifier transmits its *presentation policy* to the User (see in Figure 4). This policy includes the types of credentials it accepts and from what Issuers as well as what kind of information the presentation token must reveal from these credentials.

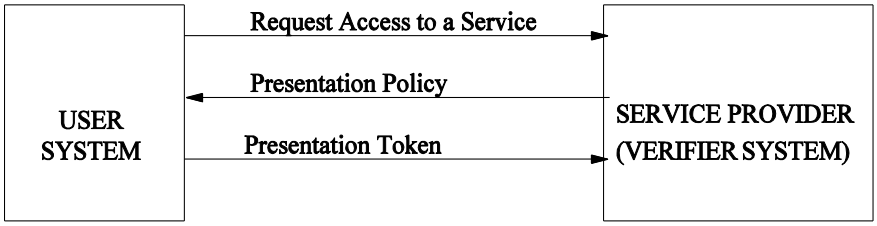

Figure 4. Authentication Protocol performed by Verifier

The User retrieves the credentials defined by Verifier's presentation policy in order to produce presentation tokens (i.e. proofs) that uncover to the Verifier, i.e. partial information about the attributes contained in the credentials. The User can combine attributes from various credentials accepted by the presentation policy. Although attributes can be of any type (e.g. integers, strings etc.) they must eventually be mapped onto integers in order to be suitably encoded into a credential. This mapping, along with the list and type of encoded credentials, is defined in the credentials specification of the Issuer. A single presentation token can contain information from any number of credentials. The token can reveal a subset of the attribute values in the credentials (e.g., IDcard.firstname = "John"), prove that a value satisfies a certain predicate (e.g., IDcard.birthdate < 1993/01/01) or that two values satisfy a predicate (e.g., IDcard.lastname = creditcard.lastname). Not only should a subset of credentials be contained in a presentation token but a presentation token evidence should be contained as well. For this reason, a User includes in the token a pseudonym, i.e. a public key generated by a user secret key. In addition to revealing information about attributes, a presentation token can, also, sign an application-specific message as well as a random nonce, if necessary, to guarantee freshness.

Upon the reception of the presentation token, the Verifier initiates the token validation process which consists of two steps. At the first step, it is determined if the content of received presentation token satisfies the presentation policy. In the second step the validity of the provided pseudonym is taken place. The authenticity of a received presentation token can be verified by using the credential specifications, the pseudonym and issuer parameters of all credentials involved in the token. This means that a service provider should obtain the credential specifications and issuer parameters in a trusted manner by the Issuer of a smart city, e.g., by using a traditional PKI to authenticate them or retrieving them from a trusted location. Since the generated presentation tokens are in principle cryptographically unlinkable and untraceable, the Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials, and that Issuers cannot trace a presentation token back to the issuance of the underlying credentials.

An application of an eBusiness model in a smart city may request a citizen to access multiple web sites, in a chain, where each site can verify that the citizen has accessed the previous, in the chain, site. This is useful in applications where the User has to visit some site before visiting another one, proving that the previous site has been visited. This can be helpful whenever two sites are in a collaboration agreement and tell to their users that if they visit both sites, the one after the other, and make some purchase they are entitled to a price reduction to the other site. In this case, the first site acting as both a Verifier and an Issuer can use the carry-over feature of Privacy-ABCs. According to this, a credential of a presentation token is issued carrying over attribute values from other credentials of the User, without, however, the Verifiers/Issuer knowing these values. Actually, we have an *issuer-oblivious* transfer of attribute values into newly issued credentials that the User can use towards another site proving the visit to the previous site which issued the carry-over credential.

Finally, another optional Privacy-ABC entity is the Inspector whose task is to uncover the true identity or some other encrypted attribute values of a specific User upon a legal mandate only. To perform this task, the Inspector first has to examine the mandate for compliance with the previously established and agreed upon by all stakeholders (including Users) *inspection grounds*. Deploying an Inspector in a Privacy-ABC system, actually, renders the system pseudonymous and not fully anonymous. However, the ultimate goal of using a Privacy-ABC system is to

provide Users with the ability to act fully anonymously as they surf the Internet using various services. The Inspector comes as a compromise between this cornerstone property of Privacy-ABCs and the legal requirement to lift anonymity upon well-established legal grounds. Thus, a Privacy-ABC system involving an Inspector entity is considered as pseudonymous only, leaving a backdoor to lifting anonymity for Users who, provably, do not comply with Verifier's and Issuers' policies or violate the law. Therefore, the use of an Inspector building block should not be a default action but should be based on a thoroughly discussed and considered decision. In all cases, the inspection grounds should be clearly indicated to Users, requiring their full, explicit agreement before issuance of their credentials. The Users should now in every detail under what circumstances their anonymity is lifted. As for the type of entity that can have the role of an Inspector, it can be any governmental law enforcement agency. We believe that this role cannot be undertaken by private sector organizations but should be under strict state control due to trust reasons.

3.1. A Scope Exclusive eBusiness Model

As we discussed in the previous sections, the main goal of Privacy-ABCs is to preserve the anonymity of the user by allowing her to generate different pseudonyms towards different verifiers. This assures unlinkability among the pseudonyms as well as between the pseudonyms and the identity of the user who generated them.

There are situations, however, where this unlinkability property among the generated pseudonyms is undesirable and, thus, it should be assured that all these pseudonyms are linked, together, belonging to the same, still anonymous, user. For example, in an online, anonymous opinion polling, users should not be allowed to bias the polling result by submitting multiple votes under different pseudonyms. In such situations, where all the pseudonyms of a user should be linked as belonging to the same, anonymous user, the verifier can request a special type of pseudonyms, called a scope-exclusive pseudonym, which is unique for the user's secret key and a given scope string. Scope-exclusive pseudonyms for different scope strings remain unlinkable. By using the URL of the opinion poll as the scope string, for example, the verifier can ensure that each user can only register, essentially, a single pseudonym to vote since all different pseudonyms are linkable as if they were one.

In our eBusiness model we encourage the use of scope-exclusive pseudonyms since we desire to have a user evaluation/reward mechanism for the information provided by each user. As mentioned above, the scope string can be the Web address of an eShop. Thus, each time a user visits the eShop and performs a transaction, e.g. recommend a product or give opinion about something she bought, she proves some things about herself, e.g. profession or age. This anonymous proof gives more credibility and importance to the recommendation or opinion, both towards the eShop and other buyers. The eShop can exploit this credibility and weight in order to shape a better marketing strategy. It may, for instance, tell the product manufacturers or sellers that users' opinions are augmented by provable credibility and weight information that can, probably, attract more buyers. This, in turn, will result in higher advertising revenue for the eShop.

In summary, according to the proposed model, eCommerce sites can exploit provable information about users in order to boost sales as well as advertising revenues. Enticing users to provide such provable information about themselves involves suitable reward and user information evaluation mechanisms. These mechanisms rely on the properties of ABCs. The users provide information about themselves in order to state opinions about products using a pseudonym to ensure

their anonymity, but their different sessions are linked to this specific pseudonym thus enabling to link the user (anonymously) to the rewards/evaluation mechanism.

4. Conclusions

In this paper we presented a generic privacy centric eBusiness model based on Collective Intelligence, that is the interactions among citizens and a smart city's facilities. This model involves users who participate in information exchanges about products, opinion sharing about products they have used, and writing evaluations of services they liked or disliked. A central element of our approach is the deployment of a new privacy enhancing technology, Attribute Based Credentials, which was proposed by the ABC4Trust project. The privacy enhancing features of this technology encourages user participation without risking their breach of privacy while they allow them to give authoritative opinions about products by revealing only elements of their eIdentities related to the opinion weight, such as their profession or expertise. This can create new marketing and business opportunities for eCommerce sites by exploiting the authoritative opinions of citizens in increasing their marketing revenues. The key element of this approach is that the buying history and consumer behaviour of the citizens will remain private while they will be able to enjoy the benefits of this new eCommerce ecosystem.

Our next step will be to implement this model along the lines in which the two ABC4Trust pilots were implemented based on the libraries provided, at no charge, at the Github code repository at https://github.com/p2abcengine/p2abcengine. The code allows easy build of the ABCs entities discussed in this paper and can provide, fast, an eBusiness environment in which real users can participate. Our approach will be to approach the municipality or Chamber of Commerce of a big city and discuss the possibility to engage a number of shops and volunteers in a pilot operation of the model proposed in this paper. Then, an evaluation phase will follow which, we firmly believe, will indicate total satisfaction of the participants. Finally, this will open the opportunity to enhance the pilot system in order to engage the whole city and its commercial stakeholders as well as the citizens as consumers.

References

[1] C.E.A. Mulligan, and M. Olsson, "Architectural Implications of Smart City Business Models: An Evolutionary Perspective", IEEE Communications, June **(2013)**, pp.80-85.
[2] A.M. Balleste, P.A. Martinez, and A. Solana, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible", IEEE Communications, June **(2013)**, pp 136-141.
[3] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, vol. 24, no. 2, **(1981)**, pp. 84-88.
[4] J. Camenisch and E. Van Herreweghen, "Design and Implementation of the Idemix Anonymous Credential System", Research Report RZ 3419, IBM Research Division, June 2002, also appeared in ACM Computer and Communication Security, **(2002)**.
[5] S.Th.Rassia, and P.M.Pardalos (editors), "Cities for Smart Environmental and Energy Futures", Springer, **(2014)**.
[6] S. Brands, "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy", MIT Press, First Edition, **(2000)**.
[7] K. Rannenberg, D. Royer, and A. Deuker, "The Future of Identity in the Information Society -- Challenges and Opportunities", Springer, **(2009)**.
[8] Z. Benenson, I. Krontiris, V. Liagkou, K. Rannenberg, A. Schopf, D. Schroder, and Y.C. Stamatiou, "Understanding and Using Anonymous Credentials", Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS 2013), Newcastle, UK, **(2013)**, July 24-26.
[9] Z. Benenson, A. Girard, I. Krontiris, V. Liagkou, K. Rannenberg, and Y.C. Stamatiou, "'User Acceptance of Privacy-ABCs: An Exploratory Study", Proceedings of the 2nd International Conference on Human Aspects of Information Security, Privacy, and Trust, Heraklion, Crete, Greece, (2014), pp. 375-386, June 22-27.

[10] S. Brands, L. Demuynck, and B. De Decker, "A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users", Proceedings of the 12th Australasian Conference, ACISP 2007, Townsville, Australia, **(2007)** , pp. 400-415, July 2-7.
[11] D. L. Chaum, "Blind Signatures for Untraceable Payments", Proceedings of CRYPTO '82, Plenum Press, pp. 199-203, **(1982)**.
[12] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps", Proceedings of CRYPTO 2004, Santa Barbara, California, USA, pp. 56-72, **(2004)**, August 15-19.
[13] J. Camenisch and A. Lysyanskaya, "Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation", Proceedings of. EUROCRYPT, Innsbrouck, Austria, pp. 93-118, **(2001)**, May 6-10.
[14] J. Camenisch and Thomas Gross, "Efficient attributes for anonymous credentials", 15th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, pp. 345-356, **(2008)**, October 27-31.
[15] J. Camenisch, "Protecting (Anonymous) Credentials with the Trusted Computing Group's TPM V1.2", Proceedings of 21st International Information Security Conference (SEC 2006), Karlstand, Sweden, pp 135-147, **(2006)**, May 22-24.
[16] F.D. Davis, "User acceptance of information technology: system characteristics, user perceptions and behavioral impacts", International Journal of Man-Machine Studies, Elsevier, Vol. 38, 3, pp. 475 – 487, (**1993**).
[17] F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, JSTOR, pp. 319 – 340, (**1989**).
[18] V. Venkatesh and H. Bala, "Technology acceptance model 3 and a research agenda on interventions", Decision sciences, Vol 39, 2:273 – 315, Wiley Online Library, **2008**.
[19] V. Venkatesh and F.D. Davis, "A theoretical extension of the technology acceptance model: four longitudinal field studies," Management Science. Vol 46, 2:186 – 204, Informs, **2000**.

Authors

Artemis Avgerou, She holds a BSc degree from the Department of Business Administration, University of Patras. Her research interests include Entrepreneurship, E-business, and Innovation and Business Modelling in the Digital Economy. Avgerou is especially interested in studying how users' social network interactions influence their attitude towards adopting new products or services and, thus, how social networking can be employed in successful e-marketing strategies.

Panayotis E. Nastou, He serves as Assistant Professor in the University of Aegean, Department of Mathematics, Samos, Greece and as Visiting Researcher in the Center of Applied Optimization of University of Florida (UFL) in USA. He worked as Senior Engineer in Computer Technology Institute (CTI), as Principal Engineer in ATMEL SA and as Auditor of Information and Communication Systems in Hellenic Data Protection Authority (HDPA). His research interests include: Combinatorial Optimization, Graph Theory, Data mining, Cryptography, Wireless Networks Security, e-Services, Agent Agreement Protocols, and Distributed Computing.

Dimitra Nastouli, She holds a BSc. In Cultural Management and New Technologies from the University of Ioannina and an MSc in Information Systems from the University of Piraeus. She is currently a PhD student at the Department of Business Administration at the University of Patras. Her interests include privacy preserving authentication methods, eCommerce and eGovernment and risk analysis of information systems.

Panos M. Pardalos, He serves as Distinguished Professor of Industrial and Systems Engineering at the University of Florida. Additionally, he is the Paul and Heidi Brown Preeminent Professor in Industrial & Systems Engineering. He is also an affiliated faculty member of the Computer and Information Science Department, the Hellenic Studies Center, and the Biomedical Engineering Program. He is also the Director of the Center for Applied Optimization. Dr. Pardalos is a world leading expert in global and combinatorial optimization. His recent research interests include network design problems, optimization in telecommunications, e-commerce, data mining, biomedical applications, and massive computing.

Yannis C. Stamatiou, He serves as Associate Professor at the Department of Business Administration of the University of Patras, Greece and Consultant on Cryptography and Security for the Security Sector of the Computer Technology Institute & Press ("Diophantus") in Patras, Greece. His interests fall in cryptography, modelling of computer viruses/worms in computer networks, cryptanalysis and ICT security with a focus in eVoting and eGovernement related security protocols and systems. He has extensive experience in theoretical and applied computer science with a focus on cryptography and ICT security.