Attribute-Based Credentials for Privacy-Aware Smart Health Services in IoT-based Smart Cities

Jose Maria de Fuentes[1], Lorena Gonzalez-Manzano[1], Agusti Solanas[2] and Fatbardh Veseli[3]

[1]Universidad Carlos III de Madrid. Spain, [2]Universitat Rovira i Virgili. Catalonia (Spain), [3]Capgemini Deutschland GmbH, Frankfurt am Main, Germany

Cities are growing as a result of the worldwide urbanization process. With the aim to become more efficient and manage their citizens' needs, governments have had to take action and, as a result, smart cities are no longer a fancy idea but a real issue in most political agendas. Most smart cities are equipped with sets of sensors and actuators that form an Internet of Things (IoT) ecosystem. IoT devices enable the collection of sheer amounts of data, which can be used to provide citizens with services in a more efficient, sustainable and economically-friendly way. Amongst those services, the provision of healthcare is especially relevant, and smart health (s-health) models have been already proposed. Despite its benefits, s-health services pose privacy problems related to the large amounts of sensitive data that they manage. In this article we advocate for the use of attribute-based credentials (ABCs) to cope with privacy issues arising from the collection of health-related data through IoT devices in smart cities. We analyze several s-health applications and show that ABCs could be properly used to address those privacy problems. With this research we set the ground for the further study and application of ABCs in smart health and other privacy-aware IoT-based smart cities' services.

Local governments struggle to provide citizens with efficient services and to transform cities into more livable places. With the aim to become smarter, cities adopt information and communication technologies (ICTs) that help them make better decisions. Thus, ICTs are the linchpin of the infrastructure that allows the transformation of cities into smart cities. Many definitions of the concept of smart city have been suggested, each of which emphasizing a specific dimension of the overall idea. A commonly accepted definition of a smart city was proposed by Caragliu *et al.*, augmented by Pérez *et al.* and served as inspiration to define the concept of smart health in [1]:

> "Smart cities are cities strongly founded on information and communication technologies that invest in human and social capital to improve the quality of life of their citizens by fostering economic growth, participatory governance, wise management of resources, sustainability, and efficient mobility, whilst they guarantee the privacy and security of their citizens"

Inspired by this wide definition, in this article, we concentrate on two of their main goals: (i) Improving the quality of life of citizens and, (ii) guaranteeing their privacy. To achieve the first goal (*i.e.*, improve liveability) we focus on the idea of smart health (s-health), which is broadly understood as the result of the natural synergy between mobile health, smart cities, IoT and big data technologies. Indeed, most smart cities use sensors and actuators that form an IoT ecosystem, which enables the collection of sheer amounts of data used for assorted services, being smart healthcare a fundamental one.

Based on the use of health data, we herein suggest several realistic solutions/scenarios that aim at improving the quality of life of citizens in their daily routines. They are focused on people with medical issues, but can be beneficial for healthy people as well (*e.g.*, relatives, doctors, etc.) However, as stated in [1] many challenges are associated to the concept of smart health in practice: being privacy protection (*i.e.*, our second goal) one of the fundamental challenges to be overcome in order for smart health, and by extension smart cities, to be a reality [2].

It is worth noting that to guarantee privacy it is not enough for every s-health service to take care of its own users' privacy. On the contrary, the collusion of providers offering several services to the same user should not allow them to learn new facts/information about the user. Thus, to pursue our second goal (*i.e.*, guaranteeing citizens privacy) we propose and discuss the use of Attribute-Based Credentials (ABCs) to protect user's privacy in several smart health scenarios.

The rest of the article is organized as follows: In Section II we briefly recall the notion of s-health. Next, in Section III we summarize the basics on Attribute-Based Credentials. In Section IV we suggest a set of representative and realistic smart health applications, and we discuss how to apply ABC to guarantee citizens' privacy in Section V. We conclude the article in Section VI with a summary of our contribution and some final thoughts.

II. Smart Health: Origins and Definition

Healthcare systems adapt to societal and political needs to achieve objectives such as, reducing costs, increasing efficiency, improving patients' treatments, reducing recovery times, etc. The healthcare sector has found in information and communication technologies (ICTs) such as the IoT an unconditional ally to undertake this process of continuous adaptation and improvement. With the adoption of ICTs, the classic paradigm of health evolved to embrace the so-called electronic health (e-health) [3]. Hence, solutions such as Electronic Healthcare Records (EHR) became commonplace. Later, the generalization of mobile devices (*e.g.*, mobile phones, tablets) opened the door to remote monitoring and telemedicine within a new paradigm of health based on ubiquity and mobility -- the so-called mobile health (m-health) was born [4].

The next technological leap that is currently influencing the healthcare sector and the society as a whole is the IoT and its inherent capability to gather unprecedented amounts of contextual data. Smart cities are one of the most apparent representatives of the emergent use of IoT and the huge amounts of contextual information that it can gather.

Smart cities seek to transform themselves by adopting technology to become greener, more efficient and sustainable, more attractive to tourism and investments and, after all, more livable. In this technological context, smart health (s-health) was proposed as a new way to use context-aware technologies, IoT and Big Data for the benefit of patients/citizens. The concept of smart health understood as:

> *"the provision of healthcare services by using the context-aware infrastructure of smart cities'"*

was proposed by Solanas et al. in [1]. However, the concept can be extrapolated to any context-aware environment where contextual data might be collected, stored and analyzed. For the sake of brevity, we point the interested reader to [1], where a detailed discussion of the smart health paradigm is provided.

III. A glimpse into Attribute-Based Credentials

The growing amount of tech-based services and applications foster the development of authentication and access control mechanisms that might threaten privacy [5]. For instance, if we use public key certificates (*e.g.* x.509), since they are linked to a key and a user's identity, all our transactions could be linked and, thus, we become traceable. To address this privacy issue, we need to guarantee that a given user is authorized to enjoy a given service or application without leaking any piece of data that is not essential to grant him/her access. We advocate for Attribute-Based Credentials (ABCs) to solve this problem.

In ABC systems, users obtain credentials (*i.e.*, some pieces of information) from an issuer. Each credential contains a set of attributes linked to the user. Based on those credentials, users create presentation tokens that are used to prove the possession of such credentials without disclosing any further information. Essentially, those are mathematical proofs that allow to attest that some properties (called predicates) are satisfied. Those tokens are sent to verifiers that check their validity before granting or denying privileges to users. For instance, a user can have the attribute `is crippled = yes' in a credential stored in an e-card provided/issued by a doctor. Then, when the user parks his/her car in a disabled-only parking place, he inserts the e-card into an e-reader to perform the verification procedure, in which the e-card computes a token that is sent to the e-reader. This token is used to attest that the user has some disability that allows him/her to park in that space, without revealing his/her specific illness or disability.

The most important building blocks of ABC systems are blind signatures [8] and zero-knowledge proofs (ZKPs) [7]. Blind signatures are a protocol in which a prover convinces the verifier that he/she owns a secret without having to reveal it [5]. ZKPs are a special form of cryptographic digital signatures, which enable a user to obtain a signature from an issuer on a set of attributes without the issuer being able to see the values of the signed attributes [9]. In terms of security, ABC systems can be classified according to the computational hardness of the mathematical problem on which they are based. In this respect, two main families can be identified: a family based on the factorization problem and another family based on the discrete logarithm problem. In this

article we consider three ABC systems (i.e., Idemix, Persiano's and U-Prove). We have chosen those systems because they are more complete (i.e., offer more properties) than others in the literature [13], and they have working implementations. and for having a working implementation. Idemix [11] is a prominent ABC system that relies on the factorization problem, whereas U-Prove [12] is based on the discrete logarithm problem [6]. Furthermore, we also consider the Persiano ABC system, which also relies on the discrete logarithm problem. Although less prominent, Persiano is relevant since it has been tailored and applied into smart cities, particularly in the transportation field [10].

In the following sections we introduce the privacy features that these systems aim to provide and we briefly describe the ABC systems described above. Although Idemix and U-Prove are based on different mathematical problems, they are similar in nature. Thus, for the sake of simplicity we present them together. Table 1 summarizes the features provided by each ABC system.

A. Privacy features

According to Rannenberg *et al.* [9], ABCs offer security because users cannot create presentation tokens unless they have the corresponding credentials and keys. Moreover, they offer privacy because these tokens do not reveal more information than the intended to be disclosed. These generic goals are further detailed into the following seven features:

- *Minimal information disclosure*: Presentation tokens do not leak any data either from the attributes to be verified nor from the remaining ones included in the credential.
- *Unlinkability*: This feature refers to two issues. First, ensuring that the use of a presentation token cannot be traced back to the issued credential (*issuance-show* unlinkability). Second, different presentation tokens cannot be linked to the same user (*multi-show* unlinkability).
- *Key binding*: If a credential contains a key protected by a user secret, no presentation tokens can be created without the knowledge of that secret. Moreover, a presentation token related to several credentials can be produced if they are related to the same secret.
- *Advanced issuance*: A new credential can be issued carrying over attributes from a former credential, while the issuer cannot learn the actual attribute values.
- *Pseudonyms*: Users can create presentation tokens containing pseudonyms that are unlinkable to each other.
- *Inspection*: Users may encrypt some values within presentation tokens. These values must be later disclosed by a trusted third party (*i.e.*, *inspector*), *e.g.* to demonstrate some malicious behavior.
- *Revocation*: When user's attributes change their value, credentials can be revoked so that no new presentation tokens could be successfully verified.

B. Persiano's anonymous credential system

Persiano *et al.* [14] proposed a method to provide users with one certificate to be used as many times as necessary (*multi-show property*) with any service provider. In a nutshell, the method has three steps. First, organizations set up the system and establish private

and public verifiable parameters. Second, each user enrolls into the system by requesting a credential and demonstrating the possession of certain attributes (anonymously). The input presented by users is their credentials and the public information previously provided by a given organization, which also verifies credentials and releases the credential certificates. Third, a user and a service provider enroll in a credential joint-proving process in which the user should prove the possession of credentials satisfying established access control policies. To do so, the user creates a set of commitments and proves their ownership constructing four ZKPs. The service provider requests a presentation token (known as *proof*) and the user returns the computed ZKPs.

C. Idemix and U-Prove

Idemix (IBM) and U-Prove (Microsoft) are two well-known ABC technologies. They have already been implemented in smart cards, which illustrates their applicability for constrained devices. Both technologies start with a setup phase, in which the issuer determines the credential specification (*e.g.*, how attributes are encoded) and provides service providers with the data to verify presentation tokens. After this phase, credential issuance is carried out every time a user needs to get a certified credential regarding an attribute. To this end, the issuer and the credential holder establish an interactive process – the user requests a credential and, if eligible, that token is computed (including a secret value) and transferred to the user. This process is carried out according to a given policy, which specifies which requirements must be fulfilled by the user to get the credential. To show that these requirements are satisfied, a ZKP is prepared by the user.

Both systems are similar in their high-level construction. However, U-Prove randomizes the signature during the issuance of the credential [15], whereas Idemix randomizes the signature during the presentation [8]. Hence, this allows more flexibility for Idemix in terms of privacy features. Presenting a U-Prove credential multiple times makes the presentations linkable to a certain credential (and indirectly to the user), whereas Idemix credentials can be randomized each time, enabling unlinkability during multiple presentations.

Table 1. Privacy features provided by each ABC technique

	Persiano	***Idemix***	***U-Prove***
Minimal info. disclosure	✓	✓	✓
Unlinkability (issuance-show, multi-show or both)	Both	Both	Issuance-show
Key binding	✓	✓	✓
Advanced issuance	x	✓	✓
Pseudonyms	x	✓	✓
Inspection	✓	✓	✓
Revocation	✓	✓	✓

IV. Smart Health Scenarios and privacy needs

We have previously stated that for smart cities and for smart health to be a reality, privacy protection is a must. To illustrate and justify this statement we have identified several s-health scenarios in which some attributes (that should be managed privately) must be proved by users. Table 2 summarizes the attributes in each scenario and their privacy needs.

A. Scenarios description

We consider three main categories to classify our s-health scenarios: (i) provision of adapted services, (ii) clearance to use services and, (iii) long-term recording services.

1. Provision of adapted services

We distinguish three classes of adapted services: mobility-oriented, energy-efficiency-oriented and accessibility-oriented (*cf.* scenarios (1) - (4), Figure1). In mobility-oriented adapted services, traffic lights could change the pedestrian crossing time depending on the agility level of users. Thus, people with children in charge (PCC), with reduced mobility (PRM) or with vision or auditive problems (PRV or PRA) might have some extra time to cross. Similarly, navigation apps (*e.g.*, Google Maps) could provide directions considering users' health status and city conditions. For example, PRM, PRV, PCC or persons with cognitive problems (PCP) may want to avoid areas such as stadiums when matches are about to start or end.

For energy-efficiency-oriented services, public infrastructures, such as hospitals, could reduce the use of illumination by adapting light intensity to the users' needs. Hence only maximum power would be applied when PRV are present. Similarly, in the class of accessibility-oriented services, elevators or billboards could adapt the size of the screen text (or the volume of audio messages) when the user proves the possession of PRV or PRA attributes.

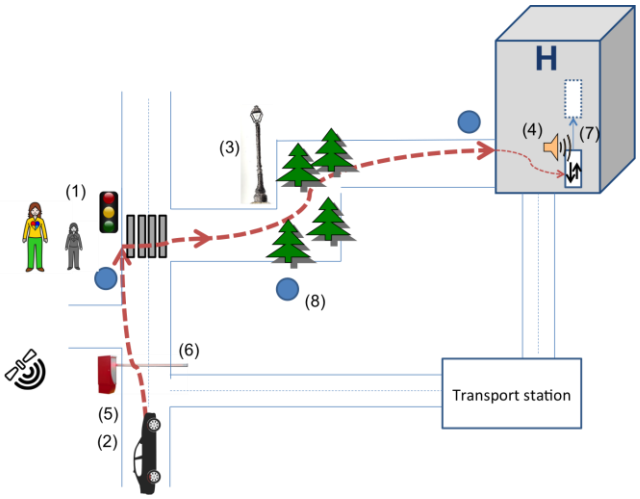

Figure 1. General overview of proposed s-Health scenarios with privacy needs

TABLE 2. Privacy issues of s-health scenarios. ***(Legend: ✓= needed || suitable, ✓* =desirable/optional || suitable with limitations, X= not needed || unsuitable.)***

	Privacy issues								***ACB technologies***		
	Attributes at stake	**Minimal info. disclosure**	**Unlinkability (issuance-show, multi-show or both)**	**Key binding**	**Advanced issuance**	**Pseudonyms**	**Inspection**	**Revocation**	**Persiano**	**Idemix**	**U-Prove**
Mobility: variable pedestrian crossing time	PRM, PRV, PRA, PCC	✓	Both	✓*	✓*	X	✓	✓	✓*	✓	X
Mobility: Adapted directions	PRM, PRV, PCP, PCC	✓	Both	✓*	✓*	✓	✓	✓	X	✓	X
Energy: Reduced lighting	PRV, PCP	✓	Both	X	✓*	X	✓	✓	✓*	✓	X
Accessibility: variable elevator/ billboards on-screen text size	PRV, PRA	✓	Both	X	✓*	X	✓	✓	✓*	✓	X
Mobility: use bus lane	PW, PUST, UAP	✓	Both	X	✓*	X	✓	✓	✓*	✓	X
Mobility: access to residential area	RRA	✓	Issuance-show	X	✓*	X	✓	✓	✓*	✓	✓
Energy: use of elevators	PRP, PRV, PRI, PCD	✓	Both	X	✓*	X	✓	✓	✓*	✓	X
Point-based habit-tracking	PUST	✓	Both	✓	✓	X	✓	✓	X	✓	X

2. Clearance to use services

These services are provided upon users attesting some medical condition. We distinguish two services: mobility-oriented services and energy-efficiency-oriented services (*cf.*, scenarios (5) - (7), Figure 1). We suggest two examples of mobility-oriented services: First, vehicles could be allowed to use the bus lane if they carry a pregnant woman (PW), or Urgent Assistant Professionals (UAP) (*e.g.*, medical emergencies personnel), or a person with a specific disease that requires high mobility priority. Second, we consider the access to restricted areas (*e.g.*, a residential area) as a service that could be granted to PRM or residents (RRA). In the energy-efficiency-oriented services, we consider the use of elevators in public infrastructures that could be accessed only if the user suffers from cardiac diseases (PCD), respiratory issues (PRI), PRM or PRV.

3. Long-term recording services

IoT and related technologies enable not only an advanced provision of existing services but also the development of new ones. In particular, a point-based pollution record could be enabled, so that some vehicle-related actions could be registered. For example, citizens who use their cars less than a given number of days per week would be given some rewards (*e.g.*, cinema tickets). Similarly, healthy actions could be registered and citizens would be rewarded too.

This scenario would be feasible as far as some entities/parties (*e.g.*, public kiosks, traffic lights) in the city were able to deliver certificates attesting those citizens healthy activities (scenario (8), Figure 1). Later, when users wish to redeem their tickets, all credentials must be provided to the verifier, who assesses the fulfillment of the established policies (*e.g.*, not having used the car more than 4 days per week).

B. Required privacy features

The scenarios described above illustrate several needs from a privacy viewpoint. For the sake of clarity, we analyze those needs (*i.e.*, privacy features) based on their initial description provided in Section III.A.

- **Minimal information disclosure**: This privacy feature is considered in all scenarios. In all cases, at least one attribute value should remain hidden but a proof that it satisfies a given property might be disclosed. For instance, the degree of mobility impairment (*e.g.*, 50% mobility limitations) or its cause (*e.g.*, arthritis) should not be disclosed to tune pedestrians crossing time. Only a proof of a certain property (*e.g.*, the user has a limitation beyond 25%) is needed.

- **Unlinkability**: Issuance-show is always needed if service providers are different to credential issuers. Moreover, multi-show is needed in most scenarios since users may show their credentials in multiple locations (*e.g.*, traffic lights, elevators) and several times. Thus, users' tracking must be avoided. However, this is not the case when accessing residential areas. In this case, physical cameras

(*e.g.*, CCTV systems) are usually in place for physical protection. With these settings, the verifier can link multiple appearances of the same user.

- **Key binding**: Depending on the scenario this property is needed to different extents (*i.e.,* mandatory, desirable or optional). It is *mandatory* in point-based habit-tracking service to prevent several users from pooling their records and obtaining better rewards. It is *desirable* in the variable pedestrian crossing time and adapted directions services, because the provided service could be different depending on the existence of multiple credentials – for example, the crossing time might be longer if the user has vision problems and he/she oversees a child. Also, this feature could be *optional* if the service provider does not require both credentials to belong to the same user. This could happen with the PCC attribute: one user could transfer it to another when the latter is taking his/her child to school. This feature is not needed in the remaining scenarios since only one credential is at stake and there is no need to use a secret to protect it.

- **Advanced issuance**: This property is needed in the point-based habit-tracking scenario since it is based on seniority. Thus, at every checkpoint a new credential could be created by accumulating previous attributes with the new one (*e.g.*, presence in a park at a given moment). In the remaining scenarios it becomes desirable since it simplifies the credential renewal – ephemeral attributes (e.g. mobility limitations) can be carried over a certain number of times before they are re-assessed.

- **Pseudonyms**: Including a pseudonym in presentation tokens is not required in most scenarios. However, for the adapted directions service, when a map service provider (*e.g.*, Google Maps) is contacted, a typical practice is to have some identifier, either transient or permanent. This enables gathering user preferences in several sessions and providing him/her with personalized services.

- **Inspection**: This property is needed in all scenarios for liability reasons. If any user performs an unlawful use of a service authorities should be allowed to disclose the identity of the user and take legal actions.

- **Revocation**: In all scenarios ephemeral attributes may come into play. This makes this feature a must. For instance, the PW attribute is not valid forever. Also, some medical issues are not permanent, *e.g.*, some mobility impairments or vision problems. Similarly, moving to another flat in a different area makes RRA to be no longer valid.

V. Applying ABCs in S-Health. The road ahead

From previous sections it might be clear that s-health scenarios in smart cities require a serious management of privacy. We sustain that ABCs are a proper tool to achieve most of these privacy requirements. Thus, in this section we analyze the suitability of ABCs for each scenario. We perform a theoretical analysis based on the privacy properties

required in each scenario and we point out some practical issues.

A. Provision of privacy features

Table 2-right shows which ABC technique is suitable for each scenario considering the offered features, shown in Table 1, and the required ones, shown in Table 2-left. It is worth noting that Idemix could be used in all scenarios, thus being the most appropriate alternative. On the other hand, Persiano can also be used in most scenarios as long as advanced issuance is not applied. However, since the point-based habit-tracking scenario requires this issue, Persiano's approach is not suitable. Similarly, it is not valid for the adapted directions scenario due to the lack of pseudonyms. Regarding U-Prove, it could only be applied to control access to residential areas because multi-show unlinkability is required in all other scenarios.

B. Practical issues

Our analysis has shown that, at least, one ABC system is suitable for every s-health scenario. However, its implementation in practice is far from straightforward. This Section highlights the enabling technologies and discusses their feasibility based on an experimental study.

1. Enabling technologies

There exists a plethora of alternatives to implement s-health solutions. For the sake of clarity, we discuss three main features: how credentials are stored, how they are verified and how parties communicate.

Regarding the storage of credentials, smartphones are a convenient choice in all presented scenarios because they are routinely carried out by most users. Alternatively, Radio Frequency IDentification (RFID) cards are also useful when the verification entity is at hand, for instance, when entering a residential area, using an elevator or looking at a billboard. Besides, the scenario involving emergency professionals (*e.g.*, police or medical doctors) may require storing the credential in the vehicle. To this end, existing in-vehicle devices referred to as On-Board Units (OBUs) could be used to handle credentials and even compute presentation tokens.

For the verification process, in most cases it is done by beacons spread throughout the city, even in the street or in a specific public place, *e.g.*, a hospital (*cf.*, blue circles in Figure 1). Moreover, traffic lights, elevators or billboards might also take the role of verifiers, thus minimizing deployment costs. Verification in remote servers is only used for the adapted directions scenario.

The communication among parties can leverage existing mobile and short-range transmission technologies. Thus, 4G/5G communications can be applied for adapted directions, whereas Bluetooth could be applied for relatively short ranges. In the case of RFID cards, Near Field Communication (NFC) technologies may be used. Finally, vehicular communications might use Dedicated Short-Range Communications (DSRC) that have been designed for their smart city use.

2. Performance results

It is important to determine whether ABCs are feasible in the proposed scenarios using computationally-constrained devices (typical in IoT ecosystems) that will be common in future s-health services. Table 3 shows the results of our analysis with the settings that we discuss next. Only those ABC techniques that have been considered to be suitable for each scenario (*cf.*, Table 2-right) have been considered in our experiments. Also, we only focus on the request and verification phases since those are the ones with more restrictive time-constraints.

For our experiments we have considered four types of devices to play the role of requester or verifier, namely a smartphone (SMT), a personal computer (PC), an on-board unit (OBU) used for communications in/out of vehicles and a roadside unit (RSU) located aside the roads to provide connectivity support. Depending on the scenario, we used the pair of more suitable devices. For instance, in the scenario where users must prove their right to use the bus lane (*i.e.*, *Mobility: use bus lane*), the requester will be an OBU and the verifier a RSU located in the street.

For each scenario (when applicable) we consider two cases depending on the used credentials. In the first case (*case A*), the credential contains the eight health-related sensitive attributes defined in our scenarios. In the second case (*case B*), credentials only include either the family-, work- or council-related attributes (*i.e.* PCC, UAP or RRA, respectively). In both cases each credential contains three additional private attributes: name, numerical identifier, and expiration date. For illustration purposes, we consider that two attributes must be privately proved to the verifier. For each case, we repeated the experiments twice, using keys of 1,024 and 2,048 bits.

The results of our experiments (*cf.* Table 3) show that Idemix is the fastest alternative (*i.e.*, lowest computational time). U-Prove is suitable in a single use case (*i.e.*, *access to residential area*) and the time of Idemix is almost equal for the verification phase and 61 and 412 ms faster in the proving phase for keys of 1,024 and 2,048 bits respectively. Although the key length affects all methods, Idemix is the one that scales better. By contrast, Persiano's approach is the slowest. However, it could be used in all scenarios except for the *use bus lane*, in which its slowness may affect the decision-making process of the driver.

VI. Conclusion

The wide deployment of sensors and actuators along with the global development of IoT ecosystems create great opportunities for smart cities and for the provision of healthcare services within context-aware environments. However, privacy issues must be taken very seriously for those services to be widely accepted by citizens.

In this article we advocate for the use of Attribute-Based Credentials (ABCs). To do so, we have recalled some of their fundamental concepts and we have proposed several smart health scenarios in which ABCs could be properly used to guarantee citizens privacy. We have shown that ABCs are a suitable solution providing challenging security features

such as unlinkability or minimal information disclosure.

Our contribution is both theoretical and practical. We have tested three ABCs approaches on four different kinds of devices. From our study, we conclude that Persiano's and Idemix are suitable ABC technologies to deal with smart city/smart health scenarios. However, due to its superior performance, Idemix is the most appropriate ABC technology in this context.

Table 3. Proving and verification time (ms) of each ABC technology per scenario with the considered devices

			Requester type	***SMT***	***SMT***	***SMT***	***SMT***	***OBU***	***OBU***	***SMT***	***SMT***
			Verifier type	***RSU***	***PC***	***RSU***	***PC***	***RSU***	***RSU***	***PC***	***PC***
Case	***Key length***	***ABC system***	Use case	Mobility: variable pedestrian crossing time	Mobility: Adapted directions	Energy: Reduced lighting	Accessibility: variable elevator/billboard on-screen text size	Mobility: use bus lane	Mobility: access to residential area	Energy: use of elevators	Point-based habit tracking
A	1,024 b	Persiano	Prove	772		772	772	341	341	772	
			Verify	358		358	303	358	358	303	
		Idemix	Prove	116	116	116	116	132	132	116	116
			Verify	94	127	94	127	94	94	127	127
		U-Prove	Prove						193		
			Verify						79		
	2,048 b	Persiano	Prove	2,356		2,356	2,356	2,502	2,502	2,356	
			Verify	2,190		2,190	1,982	2,190	2,190	1,982	
		Idemix	Prove	212	212	212	212	1,766	1,766	212	212
			Verify	302	473	302	473	302	302	473	473
		U-Prove	Prove						2,178		
			Verify						295		
B	1,024 b	Persiano	Prove	327				347			
			Verify	366				366			
		Idemix	Prove	100	100			114			
			Verify	94	106			52			
		U-Prove	Prove								
			Verify								
	2,048 b	Persiano	Prove	2,189				2,460			
			Verify	2,413				2,413			
		Idemix	Prove	169	169			1,452			
			Verify	166	413			166			
		U-Prove	Prove								
			Verify								
Device	**SMT**	**OBU**	**PC**	**RSU**							
Conf.	4-core CPU 2,26 GHz and 2GB of RAM	3-core CPU of 460 Mhz and 256 MB of RAM	8-core i7 CPU of 2.3 GHz and 8GB of RAM	2-core CPU 1,2 Ghz 2 GB RAM							

Acknowledgment

This work has been supported by the CRYPTACUS COST action (IC1403), MINECO grant TIN2016-79095-C2-2-R, and CAM grant S2013/ICE-3095. The authors would like to thank the insightful comments of the three anonymous reviewers and the editors.

References

1. A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Pérez-Martínez, R. D. Pietro, D. N. Perrea, and A. Martínez-Ballesté, “Smart health: A context-aware health paradigm within smart cities,” IEEE Communications Magazine, vol. 52, no. 8, pp. 74–81, 2014.
2. A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, “The pursuit of citizens’ privacy: a privacy-aware smart city is possible,” IEEE Communications Magazine, vol. 51, no. 6, 2013.
3. G. Eysenbach, “What is e-health?” Journal of Medical Internet Research, vol. 3, no. 2, p. e20, Apr-Jun 2001.
4. R. Istepanian, S. Laxminarayan, and C. S. Pattichis, M-Health: Emerging Mobile Health Systems, ser. Topics in Biomedical Engineering. International Book Series. Springer, 2006, ch. Preface.
5. K. Rannenberg, J. Camenisch, and A. Sabouri, Attribute-based Credentials for Trust: Identity in the Information Society. Springer, 2014.
6. Ringers, Sietse, Eric Verheul, and Jaap-Henk Hoepman. "An efficient self-blindable attribute-based credential scheme." International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017.
7. U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” Journal of cryptology, vol. 1, no. 2, pp. 77–94, 1988.
8. J. Camenisch and A. Lysyanskaya, “An efficient system for nontransferable anonymous credentials with optional anonymity revocation,” in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2001, pp. 93–118.
9. K. Rannenberg, J. Camenisch, and A. Sabouri, “Attribute-based credentials for trust,” Identity in the Information Society, Springer, 2015.
10. A. I. González-Tablas, A. Alcaide, J. M. de Fuentes and J. Montero, “Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations,” Ad hoc networks, vol. 11, no. 8, pp. 2693–2709, 2013.
11. J. Camenisch and E. Van Herreweghen, “Design and implementation of the Idemix anonymous credential system ” in Proc. of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 21–30.
12. C. Paquin, “U-prove cryptographic specification v1. 1 2011,” Microsoft Tech. Rep, 2011.
13. J. Hajny and L. Malina, “Unlinkable attribute-based credentials with practical revocation on smart-cards,” in International Conference on Smart Card Research and Advanced Applications. Springer, 2012, pp. 62–76.
14. G. Persiano and I. Visconti, “An efficient and usable multi-show nontransferable anonymous credential system,” in Financial Cryptography. Springer, 2004, pp. 196–211.
15. S. A. Brands, Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. Cambridge, MA, USA: MIT Press, 2000.

Short author bios

Jose Maria de Fuentes is visiting lecturer with the Computer Science and Engineering Department at Universidad Carlos III de Madrid, Spain. He is Computer Scientist Engineer and Ph.D. in Computer Science by Universidad Carlos III de Madrid. He has published +30 articles in international conferences and journals, all of them related to applied cryptography and privacy preservation. He is member of the Editorial board of Wireless Networks journal, as well as member of the TPC of +30 international conferences and workshops. He has participated in 6 national R+D projects and contracts. Since 2015 he has been appointed National Secretary for the Spanish mirror of ISO/IEC JTC 1/SC 27.

Lorena Gonzalez-Manzano is visiting lecturer with the Computer Science and Engineering Department at Universidad Carlos III de Madrid, Spain. She is Computer Scientist Engineer and Ph.D. in Computer Science by Universidad Carlos III de Madrid. Her research interests are on Internet of Things and cloud computing security. She has published +20 papers in national and international conferences and journals and she is also involved in national R+D projects. She is member of the TPC of +15 international conferences and workshops as well as member of Editorial board of Future Generation Computer Systems journal.

Agusti Solanas (S'03–M'06–SM'14) received the M.Sc. degree (Hons.) in computer engineering from Rovira i Virgili University (URV) in 2004, the Diploma of Advanced Studies from the Technical University of Catalonia in 2005, and the Ph.D. degree from the Department of Telematics Engineering, Technical University of Catalonia in 2007. He is a Professor with the Department of Computer Engineering and Mathematics and the Head of the Smart Health research group, URV. His current research interests include smart health, health informatics, behavior analysis, multivariate analysis, privacy protection, and computer security. He serves as a Scientific Coordinator at APWG.EU

Fatbardh Veseli has a rich international background, both in the academia and industry. He holds master's degree in information security and two bachelor's degrees, one in computer science and another in management. He is a doctoral candidate at Goethe University Frankfurt and works as a senior cybersecurity consultant for Capgemini in Germany. His previous work experience includes major European research projects in the field of security and privacy, whereas in the industry he has also gained relevant experience in the banking and software development companies in Europe. His primary research interests are privacy technologies, especially the application of cryptographic innovations for privacy respecting identity and access management systems, but also privacy assessments.

Author e-mail addresses:

Jose Maria de Fuentes: jfuentes@inf.uc3m.es
Lorena Gonzalez-Manzano: lgmanzan@inf.uc3m.es
Agusti Solanas: agusti.solanas@urv.cat
Fatbardh Veseli: fveseli@gmail.com

List of keywords:
Smart health; IoT; Internet of Things; Privacy; Attribute-Based Credentials