Trust Management in ULOOP

Carlos Ballester (Editor, University of Geneva)**, Jean-Marc Seigneur** (University of Geneva)**, Rute Sofia** (Universidade Lusófona)**, Christian Silva** (Universidade Lusófona)**, Waldir Moreira** (Universidade Lusófona)**, Alessandro Bogliolo** (University of Urbino)

This White Paper provides an insight on Trust Management within the context of the User-centric Wireless Local Loop (ULOOP) project, depicting the main principles and the overall trust management framework, and also describing its main individual components. It has as motivation to disseminate ULOOP concepts and to raise awareness towards trust management in user-centric wireless networks.

Contents

Introduction

The flexibility inherent to wireless technologies is giving rise to new types of access networks and allowing the Internet to expand in a user-centric way. This is particularly relevant if one considers that wireless technologies such as *Wireless Fidelity (Wi-Fi)* currently complement Internet access broadband technologies, forming the last hop to the end-user. This fact becomes even more significant due to the dense deployment of Wi-Fi Access Points that is common today in urban environments.

Due to such density, a relevant aspect that can be worked upon is leveraging such "wireless local-loop" by developing networking mechanisms that allow adequate resource management and a future Internet architecture to scale in an autonomic way. Such wireless local-loop could then reach rates closer to the ones provided by current access technologies, while using a lighter management infrastructure.

The EU ULOOP project [1] is investigating and implementing technology to overcome the limitation of today's broadband access technologies, expanding the backbone infrastructure by means of low-cost wireless technologies that embody a multi-operator model, i.e., a local-loop based upon what a specific community of individuals (end-users) is willing to share, backed up by specific cooperation incentives and "good behaviour" rules.

This represents a paradigm shift in the Internet evolution, as the user may be in control of parts of the network, in a way that is acknowledged (or not) by Internet stakeholders. In such scenarios where several strangers are expected to interact for the sake of robust data transmission, trust is of vital importance as it establishes a way for the nodes involved in the system to communicate with each other in a safe manner, to share services and information, and above all, to form communities that assist in sustaining robust connectivity models.

This whitepaper describes the role of trust management in the context of the ULOOP project,

All rights reserved @ULOOP consortium 2010-2013 – http://www.uloop.eu/

and how it is used to achieve security in a flexible way, without necessarily implying the use of strong security associations.

Trust Management Principles

In ULOOP, trust management and incentives for cooperation are related to understanding how to define and build circles of trust on-the-fly. Such circles of trust are capable of sustaining an environment for allowing devices to share resources in order to support the dynamic behavior of user-centric networks. Trust management is based on reputation mechanisms able to identify end-user misbehavior and to address social aspects, e.g., the different types of levels of trust users may have in different communities (e.g., family, affiliation). In situations where the created network of trust is not enough to allow resources to be shared, ULOOP devices are able to use a cooperation incentive scheme based on the transfer of credits directly proportional to the amount of shared resources.

In ULOOP, trust management and incentives for cooperation are related to understanding how to define and build circles of trust on-the-fly. Such circles of trust are capable of sustaining an environment for allowing devices to share resources in order to support the dynamic behavior of user-centric networks.

Another key aspect relates to the development and validation of a set of methods and techniques that make it possible to optimize network resources in regards to social behavior, i.e., exploiting shared interests or OSN information to create/optimize/add trust to ULOOP communities.

Notions

In ULOOP, there are two fundamental roles: *ULOOP node* and ULOOP *gateway* [2].

- A **ULOOP node** concerns a role (software functionality) that a wireless capable device takes. Concrete examples of nodes can be specific user-equipment, access points, or even some management server.
- A **ULOOP gateway** is a role (software functionality) that reflects an operational behavior making a ULOOP node capable of acting as a mediator between ULOOP systems and non-ULOOP systems – the outside world. This gateway role may or may not be owned and controlled by a ULOOP user, it may also be controlled by an access operator. The key differentiating factor of the role of gateway, in contrast to a regular ULOOP node, is the operational intelligence and mediation capability.

Similarly to ULOOP nodes, the ULOOP gateway functionality may reside in the user-equipment, in Access Points, or even in the access network. Hence, they exhibit a feature that is key in user-centric environments: their behavior as part of the network is expected to be highly variable. Gateways will be active or inactive based on several conditions such as users' wishes and network load.

From a trust perspective, we consider two additional definitions: a ***requestee*** and a ***requester*** in a trust negotiation process. A requestee in ULOOP can only be a ULOOP gateway, while the requester role can be assumed by both, a node and a gateway: nodes perform trust negotiation towards gateways; gateways perform trust negotiation among themselves.

Requestee: Requesting Trust

In ULOOP, a requester goes through four stages: i) boot up; ii) requestee discovery; iii) data transfer; iv) dispositional trust adjustment.

The ***boot-up phase*** is present in any ULOOP node, be it a requestee or a requester, since it aims to establish the initial set of conditions for the participation in a ULOOP community.

From a requester perspective, this implies generation of its ***virtual identity***. Based on this virtual identity the requester initiates the creation of a set of trust parameters, process that we name as ***dispositional trust setup***. This process will influence the way the requester is willing to cooperate with other ULOOP nodes.

Since the ULOOP trust environment may not be enough as an incentive for cooperation, the boot up phase ends up with the assignment of a set of credits that the requester may use to access shared resources.

While in idle mode, the requester behaves as any Wi-Fi node, listening passively to wireless messages (beacons) sent by nearby *Access Points* (AP) - ULOOP gateways, which may take the role of requestee. Based on collected information the requester will try to establish trust associations with one of the available ULOOP gateways via the regular MAC Layer attachment process. In other words, the requester contacts gateways available by sending, in the MAC association frames, a few parameters required to try to establish a trust association and hence, to get access to a specific service, e.g. Internet access.

Requester : Providing Trust

As previously mentioned, a requestee in ULOOP is always a gateway that may offer resources to a ULOOP node or to another gateway. The functionality of a requester has four major blocks: i) boot up, ii) cooperation request process, iii) data reception, iv) monetization and dispositional trust adjustment.

After boot-up and following the regular process of an AP, the requestee emits periodic wireless messages (beacons) announcing its presence to nodes around. As a response, the requester will send a tuple providing indications about its dispositional trust and resource thresholds. This information will allow a requester to attempt a connection with the different gateways around as part of the regular MAC Layer attachment process.

Data transmission will start with the reception of a request to send from the requester, and will proceed only if the requestee has incentives to cooperate with such requester based on the established trust association only [4].

In case the requestee is not motivated to cooperate only based on the trust association with the requester, the latter will have to send an explicit request for cooperation. After the reception of such request, the requestee will trigger a cooperation incentive scheme, which includes the negotiation of the number of credits that the requester should transfer to the requestee at the end of the transmission, in case the requester has enough credits for the requested resources [3].

Operational Example, Untrusted Environment

We start by providing a description of what occurs if an unknown node (requester) arrives to a community and wants to use some shared resources. Then the requester will send beacons aiming to setup a trust association with some ULOOP gateway (requestee), provided that: i) the requestee allows such interaction to occur (dispositional trust aspects) and; ii) there are gateways in the community which are willing to accept requested from unknown nodes to the community (dispositional trust aspects from the gateway). This process triggers social trust computation. For the case of an unknown node, this process implies that for some period of time the node will have a basic trust level which could simply relate to the provisioning of basic services, e.g. Internet access, HTTP port 80 only, and 1% of bandwidth. As this is an unknown node to the community, most likely developing trust associations will not be enough to motivate requestees to cooperate with such a new element. **Hence, it is most likely that in a scenario with unknown nodes, the cooperation incentive scheme will be triggered for any data transfer requested by a new node, until an adequate level of trustworthiness can be reached** – just looking from a trust framework perspective, this implies that the new node has to be able to somehow share resources that imply that the new element must share resources in order to see a positive change in its trust level. Another way to achieve this is through cooperation incentives [4].

Operational Example, Trustworthy Nodes

Assuming we have a well established ULOOP community, where some nodes have reached some level of trustworthiness, the dynamic conditions of a ULOOP network may lead to changes in the trust level among any pair of ULOOP devices over time. For instance, it may happen that the requestee does not have the required dispositional trust (which is adjusted over time), or the requester did not yet reach a trust level required by a particular requestee. This process triggers social trust computation, leading to an adjustment of the trust association value between requester and requestee.

After the adjustment of the trust association between requester and requestee, it may still happen that the requestee is not willing to cooperate. This may happen, for instance, if the amount of resources that the requestee has available is low, and extra incentives may be needed to associate some of those resources for the transmission requested by the requester. In this case the cooperation incentive scheme will be triggered, in order to allow requester and requestee to negotiate the credit value of the needed resources.

ULOOP Trust and Cooperation Framework

In ULOOP, trust management and cooperation incentives are related to the understanding of how to define and build circles of trust on-the-fly. Such circles of trust aim of sustaining an environment for allowing devices to share resources to support the dynamic behaviour of user-centric networks. Trust management is based on reputation mechanisms able to identify end-user misbehaviour and to address social aspects, e.g., the different levels of trust users may have in different communities (e.g., family, affiliation). In situations where the created network of trust is not enough to allow resources to be shared, ULOOP devices are able to use a cooperation incentive scheme that allows a node to gain credits in an amount directly proportional to the amount of shared resources: such credits can then be used to gain access to other resources.

Hence, trust management and cooperation incentives framework is split into three main blocks: i) Trust management; ii) Cooperation Incentives; iii) Identity management. These major blocks are illustrated in Figure 1.

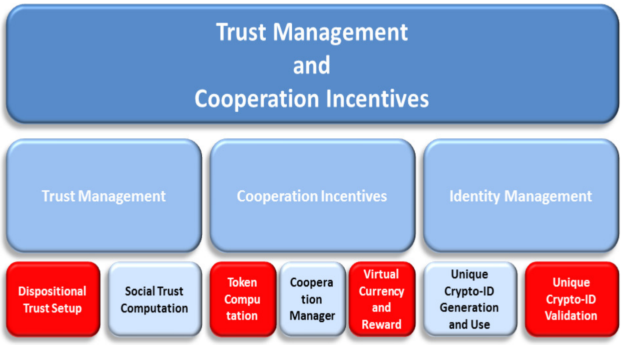
Trust Management and Cooperation Incentives
Trust Management
Cooperation Incentives
Identity Management
Dispositional Trust Setup
Social Trust Computation
Token Compu tation
Coopera tion Manager
Virtual Currency and Reward
Unique Crypto-ID Generation and Use
Unique Crypto-ID Validation

Figure 1. ULOOP Trust Framework

As illustrated, we have further split each of the blocks into sub-blocks, which correspond to different object-oriented modules as has been explained in D2.3 [5], D3 [6] and finalized lately in D3.1 [7].

The ULOOP Trust Framework can be deeply exploited to provide the cooperation incentives required to induce users equipped with Wi-Fi-enabled devices to become members of the ULOOP community and to adopt a pro-social behavior. First of all, the existence of a trust-management system that allows end-users to set their own dispositional trust level lowers the access barrier for reluctant users. Once users have become ULOOP members, the Trust Framework triggers a positive feedback by inducing each member to share his/her own resources with other members in order to increase his/her reputation that is essential, in its turn, to gain access to someone else's resources at better conditions.

Trust in ULOOP is of vital importance as it establishes a way for the nodes involved in the system to communicate with each other in a safe manner, to share services and information, and above all, to form communities that assist in sustaining robust connectivity models.

In the paradigmatic case of a ULOOP node requesting Internet connectivity to a ULOOP gateway, both the willingness of the gateway to cooperate and the service level granted to the node can depend on the trust of the gateway on the node. On the other hand, in case of multiple gateways offering the same service, the choice of the node can depend on his/her trust on the gateways. As a consequence, higher trust levels lead to more opportunities of cooperation, which, in their turn, provide the chance of further increasing the reputation of the parties involved.

Another key aspect relates to the development and validation of a set of methods and techniques that make it possible to optimize network resources in regards to social behaviour, i.e., exploiting shared interests or On-line Social Networks (OSN) information to create/optimize/add trust to ULOOP communities.

Trust Components in ULOOP

Virtual Identities: the Unique Crypto-ID

Virtual identities of ULOOP nodes and gateways are used in the process of computing and managing the set of trust associations among any pair of ULOOP devices. The goal is to mitigate the impact of impersonation and non-repudiation, while insuring the right level of privacy, e.g. by relying on PET. ULOOP considers identity-based cryptography to generate virtual identities, i.e., **crypto-IDs**. Such identity is associated to a single user, who may own more than one end-user device.

Once in place, it is more familiar for the user to manage one virtual identity and to avoid attacks based on the use of different virtual identities per user, for example, preventing voting twice. Moreover, using a unique crypto-ID avoids a potential complex process of identity disambiguation.

After the verification of the identification of a ULOOP user, the crypto-ID generated based on such identification is expected to be used across any country. To be mentioned that most countries are implementing digital identity systems to automate most of the national services. One example is Portugal, were the citizen card has embedded a chip with a one-time generated crypto-ID that is used to authenticate the used in several different services. Some services, such as changing the address information, require an extra secret key that is provided to the user with the card). This process will allow unique crypto-IDs to be generated based on any system that EU counties will decide to implement in the future to identify their citizens electronically.

In ULOOP, the crypto-id of a new node that is introduced into the system is calculated using the SHA256 cryptographic hash function producing a message digest of 256 bits over the public key of the user.

Unique crypto-IDs are generated based on a set of information extracted from the user's device, namely a public key. Such information is used to generate a unique crypto-ID based on a hash function, taken over the previous piece of information, which is implemented in any ULOOP node or gateway. The local generated crypto-ID will need to be verified by an authorized entity in order to allow the ULOOP node/gateway to gain full access to the ULOOP community. While such verification does not happen, the ULOOP device gets a minimum trust level in the community, allowing it to use a predefined set of minimum resources.

In ULOOP, owners (users) are likely to be responsible for more than one active device as previously mentioned. One of such devices is considered to be a primary device, and the remainder equipment shares the same crypto-ID generated by the first personal device, as well as the reputation level and trust associations associated to the unique crypto-ID. This is possible by using secure in range wireless or wired communications. Synchronizing the reputation levels and trust associations among personal devices will allow the user to always make use of the earned reputation level, trust associations and credits that resulted from the usage of the unique crypto-ID in another personal device. Synchronization of trust information can be done by using prior-art on file and data synchronization.

The validation of the unique crypto-ID can be done by making use of any opportunity to access the Internet (limited Internet access should be allowed by the minimum trust level). This may create some problem in extreme cases, in which Internet access is not possible for a long time. However, such scenarios are more related to delay-tolerant networks than to ULOOP. In the latter case it is expected trust management and cooperation incentives to create the conditions to make Internet access more pervasive than today.

Some user data is required for the validation: first name, last name and mobile phone number in order to be able to perform the SMS validation. Moreover the user is asked to choose a nickname that will be linked to the crypto-id. Verification near the Identity Management System will ensure the uniqueness of the nickname. The Identity Management System, owned by the Identity Validator, proves the ownership of the provided mobile phone number sending a SMS with a secret to that mobile phone number.

The ULOOP node intercepts incoming SMS messages (with a predefined format) and when recognizes the message sent by the Identity Management System, it sends back the secret received in the SMS via http together with the chosen nickname and other additional information.

If the Identity Management System recognizes that the replied data and secret are the same stored for that Crypto-Id in its database, then the validation can be considered completed and the confirmation is sent to the node together with an X.509 [8] certificate. The purpose of the X.509 certificate is to bind the public key of the node to a particular distinguished name or to an alternative name such as an e-mail address, or in ULOOP case, a ***nickname***. The node marks the Crypto-Id as validated and stores the X.509 certificate.

Dispositional Trust

Dispositional Trust (DT) is defined in ULOOP as the general willingness of a given user to trust others. As such, in a first implementation of DT, the owner of a ULOOP node will set up this value manually. The DT setup is done in the boot-up phase as explained in Section 2 and it may or may not remain the same during the node's lifetime. However, as it might provide a better protection of the ULOOP owner, depending on the surrounding environment of the node and other external factors, an adaptation process may be carried out to readjust DT automatically or after asking the user in order to protect the node's integrity. For the first implementation of ULOOP, we consider a single set-up, without changes during the trust negotiation aspect. Adaptation is an aspect that we expect to address during year 3 of ULOOP.

The dispositional trust module allows the user to configure a personal device with his/her disposition to trust other devices. If the user has multiple personal, he/she only has to set his/her dispositional trust for one device: the others will get that information from the first one when in direct contact. For the first device, the owner is prompted to set its DT, e.g. being able to select from a list of predefined values, which range from 0 to 1, being 0 "paranoid", which means that a priori the node will not trust anyone, and being 1 "blind trust", which means that the node will trust no matter what.

If the device is not the first one being configured, the user is presented with two options: i) to clone the dispositional trust level assigned to other devices that are already in ULOOP and that she/he owns, as described in D3 [6] section 2.1.4.1.1 for the usage of unique crypto-IDs in different personal devices: ii) to assign a new DT level for the node being introduced, as explained in the previous paragraph.

Since some nodes are carried by Internet end-users, their networking composition, surrounding environment and organization can rapidly change. As such, the dispositional trust level on a given node might not be appropriated in all circumstances and should be able to be adapted and changed over time, in order to protect the node's integrity. The process of dispositional trust adaptation might occur in two different cases:

- The node has a dispositional trust level that is inappropriate and leaves it too open to attacks.

- The node joins a different community to the initial one in which the dispositional trust level had been setup.

In the first case, every time a timeout occurs a social interaction analysis process is triggered, and the evidence collected together with other evidence such as QoS and attack evidence is used to determine if the dispositional trust level should be re-adjusted. This level can be readjusted manually by the user if so specified, or automatically by the system if not.
In the second case, every time the node joins a different community, the functionality checks if it is the first time that the node joins or not, and according to that, he user is prompted to specify a new dispositional trust level to use while in that community. This value could be as well automatically re-adjusted according perhaps to the social relationship with the nodes that are present (already known nodes, unknown nodes, their trust values, etc.)

Trust Computation

ULOOP considers the use of computational trust management as a complementary approach to security where a level of trust in the requesting entity is automatically computed based on different types of evidence.
Nodes are associated to other nodes by means of *trust associations,* as illustrated in Figure . A trust association T_{ij_k} is the k-th directed association between nodes i and j, and is related to the respective owner's interests and social networking perspective. A trust association holds a cost which we name as *trust level.* The trust level provides a measure of previous trust behavior, of *Quality of Experience (QoE)* of nodes, etc. Hence, two nodes may in fact hold more than one trust association among them, as represented in Figure 1, where nodes A and B hold three different trust associations: A has two trust association to node B, T_{AB_1}, which relates to the exchange of data owned by A (where A is the originator), and T_{AB_2}, which relates to the exchange of information which A is relaying (A is not the source). B has one trust association to A, T_{BA_1} with a cost of zero which e.g. could mean that B still does not trust A to relay his data. As shown in Figure 2 the different trust associations have a specific cost, and the computation of such cost is based upon the nodes expectations and beliefs.

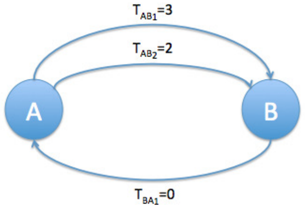

Figure 2: Social trust association examples.

The weight of a specific trust association considers *local* and *external* influences. Examples of local influences are the degree of connectivity and reputation level of node B. External influences are influences that do not relate to the nature of each node but to external networking conditions (e.g. too much overhearing probability around node B).
For instance, if Alice has the choice to connect to two nearby ULOOP gateways, Charles' gateway and Bob's gateway but she has never interacted with Bob's gateway before. Bob's ULOOP gateway is the gateway that would give her the quality of service she requires. Fortunately, she has already interacted with Charles' gateway. As she has no direct observation of Bob's gateway, therefore, she asks Charles for a recommendation. Charles has already used Bob's gateway and sends his recommendation to Alice. A third type of evidence used in ULOOP concerns reputation, which is the aggregation of different recommendations from different recommenders that are not exactly known. That reputation value may come from the aggregation of evidence external to ULOOP, for example, from the mining of existing online social networks.
The computation of trust is provided by a function implemented in ULOOP nodes and gateways[1]. Trust computation is a dynamic cost function that has to be sufficiently strong to provide, based on a local perspective, attack resistance. It comprises therefore the dispositional trust of a node, as well as evidence concerning contacts with other nodes.
One of the main challenges of the final ULOOP trust metric will be to make it attack-resistant such as resistant to the Sybil attack. To be able to bootstrap the ULOOP community, it will also be important to have a good number of users who are generally disposed to trust others. For this reason, cooperation management depicted in the next section will try to reward those users who are essential to sustain a high level of cooperation.

[1] Paper under submission.

Incentives and Rewarding

As mentioned earlier, trust allows users to seamlessly exchange services and resources without worrying about security issues. However, trust also can prevent the ULOOP communities to grow (i.e., scalability), added to the fact that it can also create disjoint communities (i.e., egoistic, better-than-others behaviour). And clearly such characteristics go against the dynamic communication found in user-centric networks.

In order to avoid ULOOP communities not to scale and the appearence of disjoint groups of users – which indeed have a negative impact in exchange of services/resources, cooperation incentives are used to allow new (and untrusted) users to join these communities and encourage users already in the trusted communities to interact with untrusted ones.

Incentives are given in the form of cooperation credits which, once earned, can be used to obtain more services/resources in other untrusted environments (or even exchanged for virtual currency as later explained in the Rewarding process in this section).

The Cooperation Manager (CM) is the entity responsible for coordinating the cooperation. We briefly explain the function of the CM and direct the reader to a more detailed view in [4]. First, CM assigns an initial amount of cooperation credits to new ULOOP nodes. Then, it controls the cooperation process among nodes (where credits are used for encouraging cooperation). CM also periodic evaluates cooperation to check whether or not cooperation took place as negotiated.

By providing new ULOOP users with an initial amount of cooperation credits, will allow them to interact with others who will see them as untrusted users. The more users cooperate, the more cooperation credits will be earned. This consequently allows already established ULOOP communities to scale and prevent the formation of disjoint communities. Additionally, the evaluation process allows for penalizing cooperation misconduct, which guarantees seamless future interactions between ULOOP users. Cooperation can take place in two different modes, namely volunteer or retailer. In the former, cooperation happens for the 'greater good' of the users and a symbolic amount of cooperation credits is exchanged between the involved ULOOP users. As for the retailer cooperation mode, services/resources are sold for an agreed amount of cooperation credits. At this point the cooperation process is further handled by the Reward Manager, which will decide whether the Requestee accepts or refuses to engage in the cooperation considering the amount of credits offered by the Requester.

This last rewarding mechanism is implemented in ULOOP to provide further cooperation incentives and to allow the ULOOP community to become part of the Internet value chain. Such a mechanism is based on a custom virtual currency system the details of which are provided in a separate document [3]. As long as ULOOP credits are used only within the ULOOP community, they work as an additional guarantee of reciprocity: the user who provides a service/resource earns ULOOP credits that can be spent later on to pay for other services/services. ULOOP credits can eventually be traded for money at the boundaries of the ULOOP community (discussing this case is outside the scope of this white paper).

Although the virtual currency system is orthogonal to the trust management system, the two systems interact with each other is three main ways. First, the trust of the requester on the Requestee acts as a discount factor, which allows trusted Requestees to pay less. Second, the trust of the requester on the Requestee increases the earning opportunities of members acting in retailer mode. Finally, the Trust Framework of ULOOP is deeply exploited in the implementation of the virtual currency system to reduce discourage cheating behaviors.

Conclusions

Trust Management in ULOOP is used to obtain security in a flexible way without the use of strong security associations. This is achieved through:

- The use of a solid trust management framework including a combination of dispositional trust levels and social trust metrics and computation.
- The use of virtual identities represented by unique crypto-IDs (one crypto-ID per user).
- Introducing cooperation incentives to complement and strengthen the trust framework and metrics.
- Introduction of rewarding mechanisms.

References

[1] EU FP7 ULOOP Project, www.uloop.eu.

[2] Rute Sofia (Editor, ULHT), Olivier Marce (Editor, ALBLF), User-Centric Wireless Local Loop Framework, EU FP7 IST ULOOP project (grant number 257418) white paper, 2011.

[3] Alessandro Bogliolo (Editor, UniUrb), Crediting Aspects in ULOOP, EU FP7 IST ULOOP project

(grant number 257418) white paper, August 2012.

[4] Paulo Mendes (Editor, ULHT), Cooperative Networking in ULOOP, EU FP7 IST ULOOP project (grant number 257418) white paper, August 2012.

[5] Rute Sofia (Editor, ULHT), ULOOP Consortium, *D2.3: ULOOP Overall Specification*. EU FP7 IST ULOOP project (grant number 257418) deliverable, September 2011.

[6] Rute Sofia (Editor, ULHT), ULOOP Consortium, *D3: ULOOP High Level Architecture Specification*. EU FP7 IST ULOOP project (grant number 257418) deliverable, December 2011.

[7] Carlos Ballester (Editor, University of Geneva), ULOOP Consortium, *D3.1: Trust Management and Cooperation Incentives Pre-Prototype Software.* EU FP7 IST ULOOP project (grant number 257418) deliverable, June 2012.

[8] R. Housley et al., Network Working Group, RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt, January 1999.

The research leading to these results has received funding from the EU IST Seventh Framework Programme(FP7/2007-2013) under grant agreement n 25741, project ULOOP (User-centric Wireless Local Loop), participants: Alcatel-Lucent Bell Labs, (FR), COFAC/University Lusófona (PT), Huawei Technologies Duesseldorf GmbH (DE), ARIA S.p.A (IT), Caixa Mágica Software (PT), FON Wireless Ltd (UK), Technische Universität Berlin (DE), University of Kent (UK), Université de Genève (CH), Level7srlu (IT), University of Urbino (IT).
For further information please visit http://www.uloop.eu/, join the **FP7 ULOOP Project** group on LinkedIn, follow **@uloopproject** and look for **#uloopproject** on Twitter.