Enabling End-to-End Secure Communication with Anonymous and Mobile Receivers - an Attribute-Based Messaging Approach

Stefan G. Weber

StefanGeorgWeber@gmail.com

Abstract. Mechanisms for secure mobile communication can be enablers for novel applications in the area of cooperative work. In this context, this article exemplarily investigates an emergency management setting. An efficient support of emergency communication is of high practical importance, but has specific challenges: unpredictable local crisis situations harden the establishment of communication structures, legal requirements dictate the use of end-to-end secure and documentable approaches, while end users demand user-friendliness and privacy protection. Dealing with these challenges, the contribution of this article is two-fold. Firstly, together with emergency practioners, we follow a participatory design approach. We define security requirements, patterns for efficient communication and derive a design proposal. Secondly, we devise a novel approach to multilaterally end-to-end secure, user-friendly attribute-based messaging for one-to-many communication. It builds on a hybrid encryption technique, which efficiently combines ciphertext-policy attribute-based encryption, location-based encryption and symmetric encryption. The hybrid encryption approach supports dynamic location attributes as user-friendly selectors for targeted messaging with dynamic groups of mobile and anonymous receivers. The achieved security of the approach and concrete application scenarios are discussed.
Key words: Attribute-Based Encryption; Attribute-Based Messaging

1 Introduction

Mobile communication has become an integral part of our modern information society. The use of personal communication devices enables the participation and cooperation of locally distributed users in a multitude of application contexts of everyday's life and work.

In some application scenarios, the availability of adequate communication facilities can even constitute a critical service: considering e.g. the case of a sudden emergency, efficient communication support can be the difference between success and failure of rescue missions, possibly between life and death of affected persons and between the loss and safeguard of infrastructure and property.

Currently, dedicated digital communication networks for emergency communications are under establishment, e.g. in Europe according to the TETRA

standard[1], promising to reliably connect organizations, parties and individuals involved in rescue efforts. Such networks require adequate security mechanisms, yet their final realization and secure use still raise a number of major research challenges. Two of these challenges are the implementation of *multilaterally secure* and *user-friendly* security mechanisms. The first objective accentuates that secure systems also need to consider possibly conflicting security goals [23], in and along with the legal and individual usage contexts. The latter one points out that "the goal (..) is not to build systems that are theoretically securable, but to build systems that are actually secure" [29] when real users deal with them in real application scenarios.

We resort to these issues, stating that the design and realization of a (mostly ideal) system for secure mobile and pervasive one-to-many communication does not only require paying attention to several explicit security requirements like mutual authentication and end-to-end encryption, but also to the more implicit security requirement of user-friendliness of the mechanisms. This paper addresses the research question, whether and how it is possible to design and realize a multilaterally secure yet practical approach that enables pervasive communication in dynamic scenarios *at ease*.

Our Contributions: We follow the approach that designing user-friendly security mechanisms requires both identifying human-adequate levels of abstraction as well as communication patterns, and realizing them in an end-to-end secure and efficient manner.

Thus, in one part of this work, we derive realistic use cases, a set of security requirements for emergency one-to-many communication and design propositions, by taking into account experiences with real users as well as legally implied security demands. Based on these findings, in the other part, we propose a novel communication mechanism: user-friendly, end-to-end secure attribute-based messaging (ABM). As a main building block, we make use of a hybrid encryption technique that supports expressive policies. Therefore, we efficiently combine ciphertext-policy attribute-based encryption (CP-ABE) [2] and location-based encryption (LBE) [26]. Applying it on the end-to-end encryption layer of the TETRA security infrastructure allows realizing the envisioned ABM scheme. Overall, the proposed concepts enable the realization of communication mechanisms that are *user-friendly*, i.e. supporting intuitive communication even with dynamic groups of mobile and anonymous receivers, by introducing location as a human-adequate level of abstraction into the selection of receivers; *multilaterally end-to-end secure*, i.e. combining privacy protection and end-to-end confidential messaging with documentation and non-repudiation means as they are required in the emergency communication domain, while also handling replay attacks on the end-to-end-encryption layer; *practical*, i.e. complying with identified emergency communication patterns, while being efficient for the use with a wide range of mobile devices.

Traditionally, end-to-end encryption layers only protect user data against confidentiality threats. Within our attribute-based messaging (ABM) scheme ,

[1] Cf. www.tetramou.com

the end-to-end encryption layer is also used as a *key management and identity abstraction layer*. While this work advances the study of secure attribute-based messaging systems, it also details practical methods for cryptographic key and access control management in large-scale distributed systems.

The remainder of this paper is structured as follows. Section 2 discusses related work. Section 3 analyses characteristics of emergency communication and sets up requirements. In section 4, we describe our approach in overview. Afterwards, details on the end-to-end encryption are given in section 5. This is followed by an introduction of the participatory design process in section 5. Our complete ABM approach is described in section 7. Our concepts are discussed and evaluated in section 8. Finally, the paper is concluded in section 9.

2 Related Work

Relevant related work on secure one-to-many messaging started with the introduction of secure role-based messaging [8, 18]. The scheme of Chadwick et al. [8] allows specifying the recipients of a message based on a single organizational role. It employs traditional public key infrastructure (PKI) [17] and role-based access control (RBAC) [25] mechanisms, but does not provide end-to-end encryption suitable to our setting, since a trusted entity is required for each message decryption. Issues related to resource-constrained devices are not addressed. The proposal of Mont et al. [18] allows combining several roles in order to form a logical policy for reader selection. The messaging scheme harnesses identity-based encryption (IBE) [12], such that logical policies are mapped to single cryptographic keys. As a main drawback, it requires frequent interactions with an online private key generator (PKG) in order to receive message decryption keys. While the authors focus on the security mechanisms for receivers, additional requirements such as documentation and non-repudiation are not addressed. In the work of Karabulut et al. [14], a one-to-many messaging service that provides end-to-end confidentiality is described. This approach harnesses IBE and also requires an online PKG. The focus of this work is to achieve an integration of mobile devices into an enterprise warehousing system. In the messaging, only a single attribute is considered. Issues related to privacy protection are not addressed. In Bobba et al.'s approach, [4], the concept of attribute-based messaging (ABM) is introduced. ABM allows logically specifying the group of receivers of a message in form of a flexible combination of multiple attributes. Thus, ABM can be seen as a generalization of role-based messaging. Bobba et al.'s approach builds on attribute-based access control (ABAC) [38] as main security mechanism and thus does not provide end-to-end encryption. After the introduction of attribute-based encryption (ABE) techniques [24, 13, 22], which provide mechanisms for fine-grained cryptographic access control, end-to-end encrypted attribute-based messaging schemes [33, 5] were proposed. Both schemes employ ciphertext-policy attribute-based encryption (CP-ABE) [2], which supports a flexible cryptographic encoding of sending policies. Especially, [5] extends the earlier work of Bobba et al. [4], by integrating encryption into the ABAC mech-

anisms, but addressed neither the handling of continuous dynamic attributes like location nor requirements related to multilateral security. Generally, the application of ABE enables a flexible specification of receivers and content by means of multiple attributes. Yet, due to the inherent use of computationally demanding pairing-based cryptography [6], the practical applicability of ABE concepts in scenarios with mobile and resource-constrained devices remains highly challenging.

The work reported in [33, 32, 7] is part of the research cycle presented in this article. In particular, we presented an initial proposal towards an attribute-based messaging scheme in the context of emergency communication. While it was limited w.r.t. efficiently handling of dynamic attributes as selectors, handling replay attacks and issues related to user-friendliness, a prototype was used to initiate discussions with real users, enabling a cognitive walkthrough[2][3] of emergency communication scenarios. This article presents a revision, major extension and follow up work on our previous research [33, 32, 7, 36, 35, 34].

To the best of our knowledge, we are the first to address the complex issue of enabling multilaterally end-to-end secure yet user-friendly one-to-many communication through attribute-based messaging in a realistic scenario under practical assumptions.

3 Communication Analysis and Security Requirements

From experiences and discussions with real users (first responders, decision makers and trainers from police and fire departments as well as relief organizations), we extracted the characteristics of emergency communications. The following lists give the main *identified communication patterns* (`CPs`) as well as the *set of security requirements* (`SReqs`) relevant to this communication.

3.1 Emergency Communication Patterns

- `CP1: Communication by location addressing:` Fast participation in a disaster response fundamentally depends on both the nature and location of a disaster. In order to handle large-scale disasters, several parties need to cooperate and communicate based on location. Some rescue efforts require the participation of local relief agencies, while others require local specialists to participate, rendering location both as a comfortable and necessary mean to select receivers.
- `CP2: Requests to unknown entities:` Some parties, like fire and police departments, are involved in most responses. But since the geographical scope of a disaster cannot be pre-determined before it actually happens, the

[2] A cognitive walkthrough, an usability evaluation method, builds on practical user experiments with a system. Being a part of a participatory design approach, it helped to understand how real users interact by and with an emergency communication system. Details are given in Section 6.

real identities of responsible people are often not directly known or available. Yet, support for efficient communication with unknown entities is required.
- `CP3: Communication with dynamic groups of entities:` When decision makers and central users need to communicate with local groups of first responders, the actual identities are also not known beforehand, or groups are even dynamically formed. These groups need to be addressable comfortably.
- `CP4: Deposition of information for future use(rs):` In many cases, information has to be deposited for entities that will join rescue operations in future.

3.2 Security Requirements for Emergency Communication

- `SReqC1: Basic security:` In emergency communication, mutual authentication, message integrity, availability and revocation of devices are basic requirements, e.g. detailed by the TETRA standard [15].
- `SReqC2: End-to-end confidentiality w/o online PKG:` Beyond that, preserving end-to-end confidentiality through encryption is legally implied for public security reasons. For scalability and efficiency reasons, the end-to-end encryption mechanism also shall not rely on an online private key generator (PKG).
- `SReqC3: Protection against replay attacks:` Means that protect against replay attacks are required, in order to prevent an attacker from injecting a valid message a further time.
- `SReqC4: Non-repudiation of senders:` Emergency communication requires to document who sent which messages.
- `SReqC5: Documentation of readers:` Also, the parties and entities who read received messages, requests and commands need to be documented for post-hoc audit purposes.
- `SReqC6: Efficiency of security mechanisms:` Employed security mechanisms need to be suitable for resource-constrained mobile devices that are widely used in emergency communications. Especially, a real-time communication must be possible.
- `SReqC7: User-friendliness:` In order to foster end user acceptance, security mechanisms must be understandable by and appropriate to casual users [11], i.e. user-friendly. For senders of messages, this implies minimum learning efforts as well as an intuitive use.
- `SReqC8: Receiver anonymity:` Many persons involved in responses, like specialists, doctors or volunteers, are only available on requests sent to their mobile communication devices. Yet, the individual participation depends on the compatibility with individual privacy preferences. Especially, many receivers demand privacy protection in the form of receiver anonymity, while being available for location-based addressing and participation in rescue missions.

We stress that the envisioned communication functionality requires dealing with conflicting security requirements. In particular, receiver anonymity has to

be reconciled with secure communication and non-repudiation goals. In the sense of multilateral security, we strive for a solution that fairly balances these inherent tradeoffs. The arising research challenge that we thus address is summarized in Figure 1.

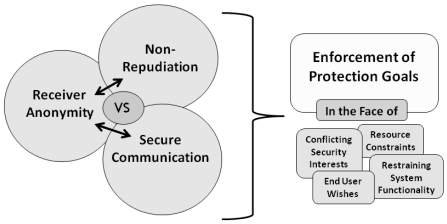

Fig. 1. Challenge

4 Our Approach in Overview

The last section elicited requirements in order to detail the central research question of this article: how to enable a sender to securely and comfortably communicate with unknown receivers, that may locally form dynamic groups? This section introduces our proposed solution.

As motivated earlier, reaching the right actors at the right time is of high practical importance for the coordination of incident responses. However, in the beginning of a response mission, the communication structures are often little established.

In particular, a sender in such a messaging task does not immediately known the *identities* of the parties and entities she aims to communicate with. Rather, the sender can elaborate *which kind* of organizations, roles and specializations are appropriate and *where* the receivers should be present, to allow for a fast engagement [30, 16].

Thus, we propose that a sender may specify the group of intended readers of a message on a level of abstraction different to identity. Instead, the sender may leverage a specific logical combination of receivers' properties. Especially, we propose to use a set of *logical attributes*, as depicted in Figure 2, in conjunction. It consists of attributes related to an organization, a role, a specialization and/or a location, i.e. a place where the receiver is currently present. Such a combination is what we call a *logical messaging policy*. It is used to specify the group of readers of a message that is to be sent to the outside world and, in particular, towards an incident site.

Communication mechanisms that support a flexible specification of readers via an attribute-based description are denoted as attribute-based messaging

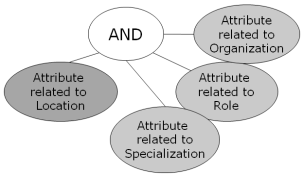

Fig. 2. Structure of logical messaging policy

(ABM) in the research literature [4, 33, 5, 36]. ABM concepts potentially allow implementing a communication approach that handles all major communication patterns, as given in Section 3.1; ABM thus could also minimize learning efforts for the senders.

In particular, we propose to realize end-to-end secure attribute-based messaging according to the following main steps (cf. Figure 3):

1. The sender selects the group of intended readers by specifying a conjunction of attributes that readers have to fulfill, encrypts the message under the resulting *logical messaging policy* using an appropriate encryption technique and broadcasts it to all mobile users that are logged in a given communication network.
2. Every receiver locally evaluates every received message on her communication device. The encryption mechanism has to assure that she can only decrypt a message and thus only read it if she satisfied the specified attribute combination.
3. Every reader of a message sends an acknowledgement to the sender, i.e. she confirms that she read the message. Thus, the sender does not know the actual group of readers of a message when sending it, but only after receiving the acknowledgements.

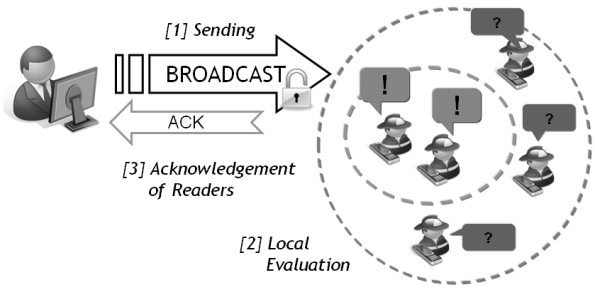

Fig. 3. Steps of attribute-based messaging

The approach, as introduced, leverages a variant of an implicit addressing mechanism [20, 21], which makes use of attributes for addressing mobile users, in order to retain a functionality for targeted communication and protecting receiver anonymity at the same time. In order to achieve this capability, we propose that a mobile user is associated with a set of attributes that she satisfies. The attributes in use can be classified into two classes: static and dynamic. The values of static attributes do not change over time, e.g. a mobile user belongs to the same organization and has the same role as long this is not changed due to external reasons. Dynamic attributes possibly exhibit a frequent value change, e.g. the current location of first responder changes as she moves. The present proposal requires handling dynamic and static attributes on the encryption level[3].

In order to realize the end-to-end secure ABM functionality, we can also build on existing digital emergency communication networks, e.g. harness the existing TETRA security infrastructure. As such, the network provides basic security services for emergency communication; it also implies the existence of secured mobile devices on the receiver side. Yet, realizing the end-to-end encryption leads to new challenges: traditional asymmetric encryption schemes and PKI concepts are not practical for communication with unknown receivers. In addition, existing encryption techniques do not provide the required flexibility and means for handling dynamic attributes with continuous values, e.g. location. To overcome these issues, we propose to leverage ciphertext policy attribute-based encryption (CP-ABE) [2]. This is a recent asymmetric certificate-less encryption technique that directly supports a cryptographic realization of flexible *attribute*[4] *policies*. Yet, CP-ABE has practical limitations w.r.t. the handling of dynamic and continuous attributes. Thus, an extended encryption technique that may also handle dynamic attributes is required.

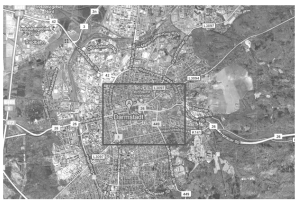

Fig. 4. Location selection on digital map

[3] One-to-many communication is crucial for first response scenarios. Typically, it is supported on the network layer. E.g. in TETRA networks, multicast communication mechanisms are described. However, these mechanisms do not specify the end-to-end encryption [15].

[4] Note that the cryptographic attributes of CP-ABE techniques are not equal to the logical attributes/selectors of ABM schemes, but belong to different conceptual layers of the messaging system.

In the emergency response domain, the use of augmented digital maps is inherent [9]. An integration of the selection of location attributes into a digital map was proposed by real users to support an intuitive use (cf. Figure 4 and Section 6). It requires an expressive encryption, for incorporating location into the end-to-end encryption. Due to the local evaluation of policies, receivers can be addressed depending on their current location, without requiring them to continuously provide location information beforehand[5].

5 Realizing the End-to-End Encryption Layer

In this section, we introduce important building blocks of our work, namely the employed encryption techniques and their integration with the TETRA security architecture.

5.1 Ciphertext Policy Attribute-Based Encryption

Attribute-based encryption (ABE) [24] is an encryption technique which generalizes the functional role of identities and keys. In traditional asymmetric encryption schemes, identities relate to distinct public key / private key tuples. In ABE, both public key and private key concepts are replaced by *sets of attributes*, which abstract from actual user properties. Moreover, ABE is certificateless and the cryptographic credentials are issued by a central trusted party called *attribute authority*, which is in possession of a global *master key* for key generation. Since users are associated with sets of attributes, they might try to trade some attributes and related private key components to gain more decryption powers. However, ABE systems are *collusion resistant* [2], i.e. keys of different users are incompatible due to the cryptographic construction. Like identity-based encryption, ABE cryptographically builds on pairings [6], i.e. bilinear maps that provide an extra structure on special elliptic curves. While pairings enable attribute-based encryption, they are inherently computational demanding. From a practical point of view, the goal is to minimize pairing-related operations, in order to enable use on resource-constraint devices.

Ciphertext policy attribute-based encryption (CP-ABE) [2] is a particular variant, which associates a set of attributes used in the encryption process with logical access structures[6], also called *attribute policies*. Thus, the encryption algorithm takes as input a message and an attribute policy. The algorithm encrypts the message and produces a ciphertext, such that only a receiver possessing a set of attributes that satisfies the attribute policy is able to decrypt that message. In the following, we assume that the ciphertext implicitly contains the policy. In practical applications, CP-ABE is used as *hybrid encryption*: a message itself

[5] The continuous provision of location information would require further mechanisms for privacy protection (cf. [31, 37]).

[6] Due to the use of Shamir secret sharing [27], the access structures are trees with nodes that represent t-out-of-n combinations of attribute child nodes, naturally including conjunctions (n-out-of-n) and disjunctions (1-out-of-n).

is encrypted with a random symmetric secret key. Only this *session key* is then CP-AB encrypted under a policy. An example of an CP-ABE policy containing attributes that are taken from the emergency management domain and its application to encryption in hybrid mode is given in Figure 5.

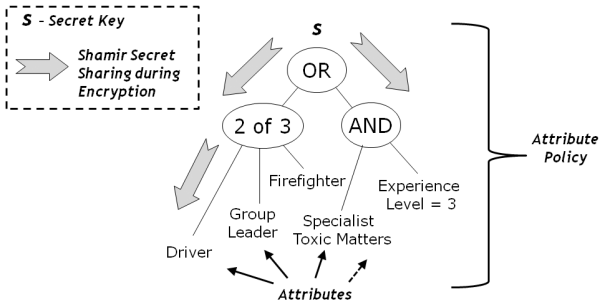

Fig. 5. Example of CP-ABE policy

CP-ABE concepts can be the basis to realize a combined cryptographic *key management and identity abstraction layer*, which makes them interesting for the use in messaging applications. However, CP-ABE alone is practically inefficient for handling dynamic attributes, i.e. attributes that change their values of time, with continuous values, like location.

5.2 Location-Based Encryption

The concept of location-based encryption (LBE) according to [26, 10] aims at securing mobile communication by limiting the area inside which the intended recipient can actually decrypt a received message. In order to implement this functionality, it adds a layer of security to the symmetric encryption of a message: the session key is combined with the targeted reader's geographic location L, producing a location-locked key, which is then sent along with the encrypted message.

As a result, the ciphertext can only be decrypted if the session key can be recovered from the location-locked key. In turn, LBE requires that this is only possible if the receiver's device is physically presented at location L, or respectively inside an geographic area associated with L. Technically, location verification hinges on a tamper-resistant GPS receiver inside the receiver's mobile device.

In LBE, the sender has to transmit parameters which define the area where decryption is permitted and may specify additional dynamic constraints like time periods or receiver velocity that have to be verified upon decryption [1]. In general, location-based encryption techniques require an efficient mapping from location areas to symmetric keys, which is called *location lock* in the following.

5.3 Hybrid Encryption Technique for Expressive Policies

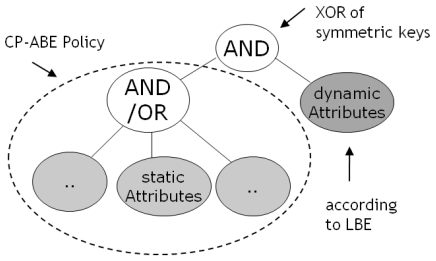

Fig. 6. Construction principle of hybrid encryption technique

In this section, we describe an efficient hybrid encryption technique that supports expressive policies. The technique is hybrid, as it combines CP-ABE with LBE on the level of symmetric keys (cf. Figure 6). It supports encryption under expressive policies, since it can efficiently handle logical attributes with continuous values, like location[7]. We use the following notation:

- $L^{(P_1,P_2)}$ specifies an geographic area with the shape of an rectangle, defined by GPS coordinates $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ (cf. Figure 4, which exemplarily shows the definition of GPS coordinates on a digital map.). In the following, we also denote $L^{(P_1,P_2)}$ simply as L.
- $E_{AP}^{L^{(P_1,P_2)}}(M)$ denotes the encryption of a message M under a logical conjunction of a CP-ABE attribute policy AP and a LBE location area attribute $L^{(P_1,P_2)}$.
- $D_{\{A\}_R}^{P_R}(CT)$ denotes the decryption of a ciphertext CT initiated by a receiver R, using his private attribute set $\{A\}_R$, while being positioned at GPS coordinate $P_R = (x_R, y_R)$.

It is possible that one of the two main parts of a policy remains undefined:

- In case the CP-ABE part AP is not specified, encryption is reduced to location-based encryption;
- In case the LBE location area attribute $L^{(P_1,P_2)}$ is not specified, encryption is reduced to ciphertext-policy attribute-based encryption.

We describe the comprehensive approach in the following. In general, decryption succeeds if a receiver's (R) attribute set $\{A\}_R$ satisfies the attribute policy AP and R is positioned within $L^{(P_1,P_2)}$, i.e. if $x_2 \geq x_R \geq x_1$ and $y_2 \geq y_R \geq y_1$ hold. Figure 7 shows the basic schemes of the encryption technique in overview.

[7] We restrict the description to location, however, further continuous attributes can be handled analogously.

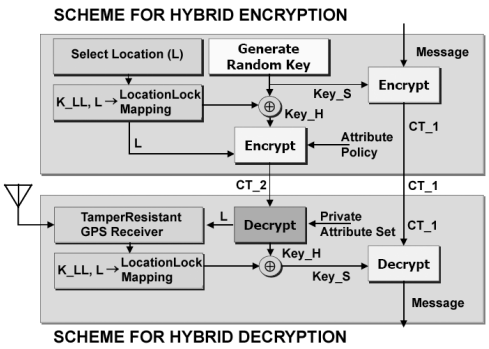

Fig. 7. Schemes for encryption and decryption

The proposed hybrid encryption employs a keyed *location lock mapping*, denoted as $f_{LL}(L^{(P_1,P_2)}, K_{LL})$, according to the following principle: GPS coordinates P_1, P_2 and K_{LL} are concatenated. Then, the resulting string $s_{LL^{(P_1,P_2)}} = x_1||y_1||x_2||y_2||K_{LL}$ is hashed, $h(s_{LL^{(P_1,P_2)}})$, to a bit string that matches the chosen key size, in order to produce the location lock value[8].

Scheme for Hybrid Encryption The *hybrid encryption scheme* proceeds as follows (cf. Figure 7, upper part):

1. A random session key Key_S is generated.
2. The message is symmetrically encrypted under Key_S, producing ciphertext CT_1.
3. The location lock value is computed from the selected location area L and key K_{LL}.
4. Key_S is XORed with the location lock value, generating a hybrid key Key_H.
5. Key_H is concatenated with an encoding of the location area L, producing the string $L||Key_H$. This string is CP-AB encrypted under an attribute policy AP, producing ciphertext CT_2
6. CT_1 concatenated with CT_2 represent the ciphertext CT. CT is transferred to a receiver R.

Scheme for Hybrid Decryption The *scheme for hybrid decryption* proceeds as follows (cf. Figure 7, lower part):

1. After reception of $CT = CT_1||CT_2$, receiver R tries to decrypt CT_2, using his private attribute set $\{A\}_R$. On successful decryption, the location area L and Key_H are recovered.

[8] In this operation an appropriate collision resistant hash function has to be employed. Assuming e.g. a level of 160 bit security for symmetric keys, then SHA-1 is a hash function of choice.

2. R's current GPS position P_R is computed by means of a tamper-resistant GPS receiver and verified to be inside the location area L. On success, the location lock value is computed, taking L and key K_{LL} as input parameters.
3. The location lock value is then XORed with the recovered Key_H, in order to reconstruct Key_S.
4. Key_S is used to symmetrically decrypt CT_1 to M.

5.4 Integration with TETRA Security Architecture

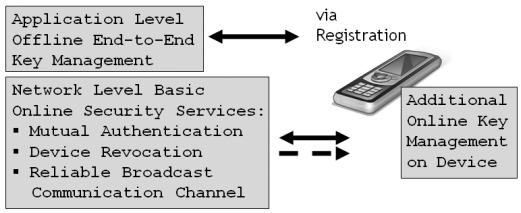

Fig. 8. Security services of communication network

TETRA (Terrestrial Trunked Radio System) is an open standard for digital radio [19]. It has been adopted for emergency communication by a number of national European administrations. It was especially designed with security as one of its principal features, including mutual authentication, air interface encryption and disabling of mobile devices. However, in its basic form, it only protects the air interface layer. Thus, additional, end-to-end encryption mechanisms are required for application contexts with end-to-end confidentiality requirements. The end-to-end encryption key management is in the user domain, especially, the underlying key management infrastructure is unable to decode end-to-end encrypted messages or access the end-to-end keys.

For the receivers, we assume that they are equipped with mobile communication devices, that provide a digital communication channel to operational headquarters and command and control centers by means of TETRA. The mobile devices are uniquely identifiable and equipped with dedicated smart cards including TPM chips, rendering them practically tamper-resistant. End-to-end encryption keys are individually issued, e.g. along with the distribution of these devices.

In the following, we focus on broadcast-based one-to-many communication between a sender in a control center and mobile receivers. Since the TETRA communication infrastructure does not provide confidential point-to-point channels, we propose that end-to-end security of broadcasted messages is guaranteed by means of end-to-end encryption layer security mechanisms.

6 Supporting User-Friendliness

The design of our ABM approach proposal draws from experiences and discussions with potential real users, i.e. first responders, decision makers and trainers from police and fire departments as well as relief organizations. This dialogue was part of a participatory design process. We discuss the user study as well the impact on the design decisions in the following sections. In particular, we introduce the setting of the user study, describe the experiments that were executed by the participants and shortly elaborate on received user feedback.

6.1 Design Process

The design process (cf. Figure 9) of our proposal to end-to-end secure attribute-based messaging followed an iterative approach:

- We presented our initial proposal of an attribute-based messaging scheme and system for end-to-end confidential emergency communication both to the IT security research community (e.g. in [33]) and to the emergency management research community (e.g. in [32]).
- The associated prototype was used to initiate discussions and to conduct a user study with potential real users, based on a cognitive walkthrough [3] of typical emergency communication scenarios. The experiments helped to understand how potential real users prefer to interact by and with an emergency communication system and ABM concepts, in particular.
- The findings of the study contributed to Section 3 and to the proposed ABM design and concepts, as presented in this article.

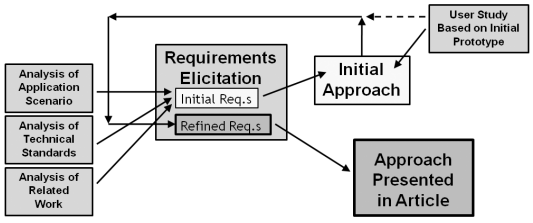

Fig. 9. Iterative, participatory design process

Setting Our study was organized as an one-day end user evaluation session. During this session, potential real users and emergency management domain experts were confronted with the prototype, written descriptions as well a moderator. In particular, the population included emergency workers and decision makers of fire brigades, lectures and decision makers of police authorities[9].

[9] Our study particularly related to *German* emergency workers.

Each participant was given a printout of the documentation of the study as well as a brief oral introduction to the concept of attribute-based messaging and its proposed application to the area of emergency communication by a moderator. The participants were seated at a table. A computer screen on the table and a keyboard and a mouse were provided as input devices. The documentation of the experiments and discussions was supported by a minute writer.

6.2 Experiments

During the study, the domain experts were requested to participate in a particular cognitive walkthrough of emergency communication scenarios. Each participant was confronted with an ABM prototype that supported a flexible definition of sending policies. In the proposed setting (cf. Figure 10), the messaging policies were not restricted to a certain logical structure. Instead, arbitrary conjunctions and disjunctions could be used to specify the intended readers. For the definition of policies, the participants were also supported by an editor that helped to define nested policies (cf. Figure 10).

After the introduction, the participants were asked by a moderator to execute several messaging acts and define appropriate policies. The prototype visualized the message exchange as well as the particularly chosen readers. Afterwards, the users could elaborate on the mental and cognitive processes and difficulties and formulate wishes on the design.

In particular, the experiments included

- executing messaging acts suitable for pre defined situations,
- defining a messaging act that was known to be common due to personal experience,
- defining a complex, yet still realistic messaging act.

After executing the tasks, the participants were requested

- to answer questions on their ability to handle the selection of readers by means of attribute combinations,
- to elaborate on the comprehensibility of the proposed communication concept,
- to identify elementary as well as difficult operations,
- to compare the proposal with known means for emergency communication,
- to state personal preferences for the usage of an ABM system.

6.3 User Feedback

In the following, we present selected quotes that were given by the participants:

- "This is a charming way of addressing communication partners that are not known by identity."
- "The approach is in accordance to our existing role- and task-based ICT."
- "ABM is very useful to communicate with external specialists."
- "Selecting location attributes directly on a digital map would be favorable".

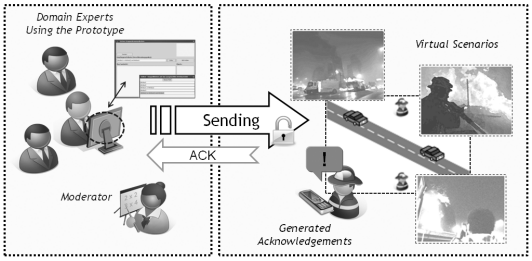

Fig. 10. Setting of experiments

6.4 Implications

The overall approach was recognized as a generalization of the concept of messaging lists, that is common in emergency communication. Thus, ABM was considered as applicable to the targeted setting and understandable by the available group of experts.

In general, attribute-based messaging was considered to be easy learnable, given that messaging acts can be handled by policies that are easy definable. Using disjunctions and conjunctions within one policy was considered too complex and too difficult. Thus, for the design of messaging policies, a compromise of expressiveness and complexity was favored. Additionally, a selection of location attributes directly within a digital map was an articulated end user wish, in order to support an intuitive use. Instead of using the proposed editor for defining policies, drop-down boxes with lists of attributes were preferred.

The received feedback was incorporated into the final design of our attribute-based messaging approach, as presented in this article. In the present design, also the resource constraints imposed by the mobile devices that commonly used for emergency communication are considered.

7 Approach to Attribute-Based Messaging

In this section we describe the technical details of our ABM approach in conceptual and schematic views.

7.1 Conceptual View

Within a comprehensive system for ICT-based emergency management, the communication mechanism of end-to-end secure attribute-based messaging is implemented in a module for outgoing communication as well as on personalized communication devices that are carried by the mobile receivers. The module for outgoing communication provides

– a digital map (DM), that helps selecting location attributes,

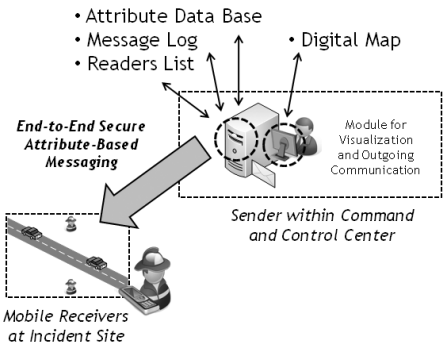

Fig. 11. Implementation of ABM

- a central attribute data base (ADB), that stores all defined static attributes,
- a message log (ML), that stores outgoing messages,
- a readers list (RL), that is used to document the group of readers of a message.

Log and list are append-only. Figure 11 shows the components in overview.

In the present approach, the realization of end-to-end secure ABM hinges on two main conceptual layers:

- On the *logical messaging policy layer*, a sender may specify logical messaging policies (see Figure 12 for a simple example), in order to select receivers in the communication via an ABM system on a level of abstraction different to identity.
- The *access control layer* provides security mechanisms that enforce the constraints specified by the logical messaging policies, by employing encryption techniques and tamper-resistant access control support mechanisms.

In the following, sending a single message by means of the provided communication functionality is called a *messaging act*.

7.2 Logical Messaging Policy Layer:

In any messaging act, a sender

- has to choose between two communication modes: *direction communication / requests* and *depositions*. The first one refers to the communication patterns `CP1-CP3`, the latter one to `CP4` (cf. Section 3.1);
- specifies the logical messaging policy. Therefore, the sender firstly selects attributes that represent organizations (e.g. Police), roles (e.g. Group Leader) and specializations (e.g. Specialist Toxic Matters), from the central attribute database, secondly, selects a location attribute by selecting a geographic area on a digital map. This is executed by selecting two points P_1, P_2 that define

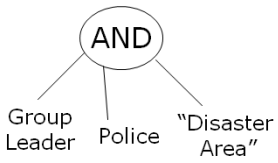

Fig. 12. A simple policy

a rectangle (cf. Figure 4). According to the spatial position on a digital map, each point refers to a GPS position that is thus specified.

The basic structure of logical messaging policies, as shown in Figure 2, is a logical conjunction of one attribute related to location, one attribute related to a specialization, one attribute related to a role as well as one attribute related to an organization. Thus, a specified logical messaging policy consists of at least one and at most four of the given attributes.

7.3 Access Control Layer

End-to-end secure attribute-based messaging requires an efficient end-to-end encryption mechanism in order to guarantee end-to-end confidentiality. For this purpose, we make an efficient use of the hybrid encryption technique described in Section 5.3. It is thus a main mechanism for implementing the access control layer.

Yet, the selection of the communication pattern has an effect on this access control layer:

- for direct communications (`CP1,CP3`) and requests (`CP2`), the enforcement requires making use of the hybrid encryption technique,
- depositions (`CP4`) can be handled with CP-ABE (cf. Section 5.1) alone.

In the latter case, the specification of sending policy does not contain a continuous location attribute. This allows for a direct mapping to CP-ABE policies[10]. If a deposition is chosen, also no broadcast of messages is executed. Rather, the deposited message is internally stored on the ML for parties that join the rescue missions at a later point in time.

The following descriptions focus on the realization of `CP1-CP3`. In this case, logical messaging policies are mapped to the hybrid encryption technique as follows, also shown in Figure 13: the attributes related to organizations, roles and specializations are mapped to a structured CP-ABE policy. This structured policy adheres to the structure of the messaging policy, i.e. it is a conjunction.

[10] Yet, this kind of encryption can be executed in the same technical setting given by our hybrid encryption approach, i.e. the hybrid encryption technique reduces to CP-ABE in that case.

The attribute related to location is basically handled as introduced in Section 5.3. In particular, a key is securely derived from GPS coordinates and then XORed with a symmetric session key.

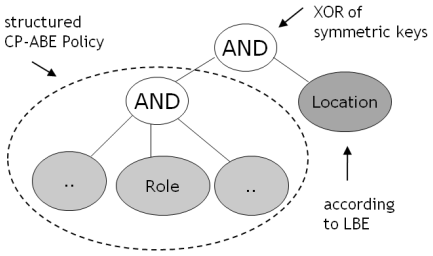

Fig. 13. Mapping of messaging policies to hybrid encryption

7.4 Protocol for End-to-End Secure Messaging

This section provides a schematic view of messaging acts, in order to complement the description.

In order to send a message, the sender has to specify a logical messaging policy by selecting static attributes and a location attribute on the digital map DM, and composes the message content. Basically, a messaging act furthermore consists of a broadcast of an end-to-end encrypted message M_{E2E} and answer back steps. The end-to-end encryption incorporates a unique message ID, ID_M, to prevent replay attacks, symmetric non-repudiation is supported by message authentication codes (MACs). Messages sent out and acknowledged readers are documented on message log (ML) and readers list (RL). Optionally, readers can reply and answer a read messages.

In Section 4, our approach to attribute-based messaging has been introduced to consist of the main steps *sending*, *local evaluation* and *acknowledgement*[11]. The protocol that implements these steps and which is underlying every messaging act is depicted in Figure 14. In this figure, the left side represents the sender in a control center, the right side the mobile users that receive message. Here, $||$ represents string concatenation. In detail, the protocol proceeds as follows:

– The sender concatenates: a message content m, a unique message ID, which we denote as ID_M, and a MAC on the former two contents. This MAC is realized via hashing the concatenated content and a symmetric key. Then, an encryption according to the specified logical messaging policy is executed.

[11] Optionally, a reader can answer a message. This step can be implemented mostly analogously to acknowledgements. Further details, e.g. a set of reference strings for indicating different levels of priority of a message, are considered future work.

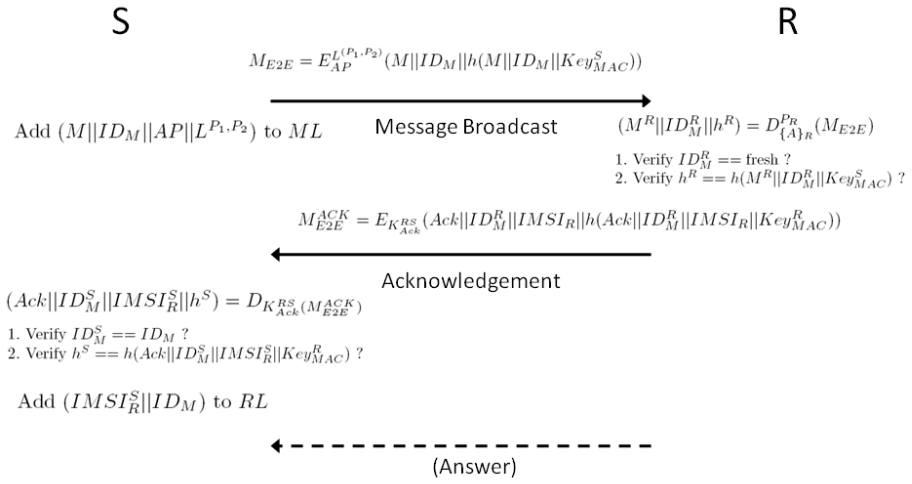

Fig. 14. Protocol for end-to-end secure attribute-based messaging

The so encrypted message M_{E2E} is broadcasted via the digital emergency communication network. Also, the message is added to the message list ML.

- Upon receiving the message, every mobile user tries to decrypt the message. This succeeds, if the policy is satisfied. Decryption provides the received message content M^R, the received message ID IM_M^R as well as the received MAC value h^R. Every user verifies whether the message ID is fresh, i.e. that it has not been used before[12]. Also, it verifies the MAC by recomputing it and comparing the value.
- In case both verifications succeed, a receiver becomes a reader of the message. She acknowledges that she is able to read a fresh and integrity protected message. In order to so, she concatenates the string "Ack", the received message ID, her unique device identification number and a MAC on the previous content. Together, this is symmetrically encrypted and sent to the command and control center as acknowledgement message.
- The sender decrypts every received acknowledgement message. Decryption provides the "Ack" string, the value of a message ID ID_M^S, a devices identification number $IMSI_R^S$ and a MAC value h^S. The sender identifies the messaging act via the ID_M^S and verifies the MAC value. If this succeeds, a reference to the reader and the message is added to the RL, in order to document the group of readers of a message.

[12] In order to verify that a message ID has not been used before, a receiver has to store every received message ID locally on her device. The received MACs are also stored to support a later analysis.

7.5 Examples

As introduced, end-to-end secure attribute-based messaging is a very flexible communication mechanism. In this section, we give concrete examples of messaging policies and elaborate on their relevance to the first response application context, in order to show how ABM can be applied effectively. In Figure 15, six distinct examples are given. In every example the rightmost string shall represent a location attribute selected on a digital map. Here, textual representations instead of GPS positions, e.g. "Near Disaster Area", are used to convey the functions in the application context.

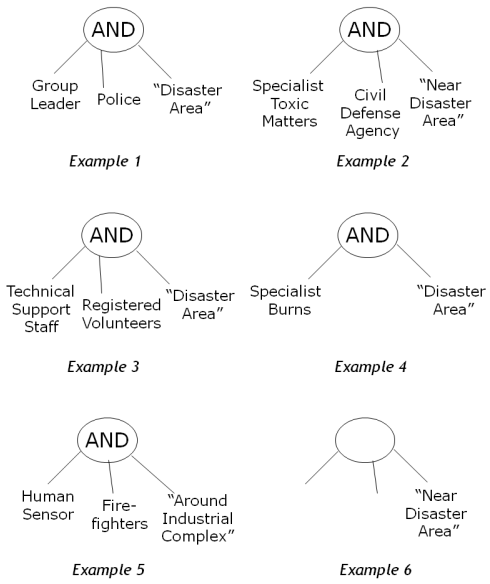

Fig. 15. Examples of logical messaging policies

- *Example 1:* This policy can be used in order to communicate tactical information relevant to a rescue mission. The role attribute *group leader* is used to address mobile users with command and control responsibilities in the field. This reflects that command and control is actually exercised locally in the first response domain.
- *Example 2:* Based on a policy as given in this example, specialist that may immediately be required can be contacted. In this case, the sender can select a location attribute that specifies a region which allows for a fast transfer to the incident site.

– *Example 3:* This policy maps to a situation, which requires large numbers of helpers with a special skill. Such helpers are normally not directly associated to an emergency services organization, but are rather available and organized as volunteers. In the message content, they can e.g. be requested to show up at a certain point, where a local organizer will arrange further instructions.
– *Example 4:* Medics with special skills are often required in order to quickly react in emergency situations. With such kind of messaging policy, they can efficiently be contacted to allow for a fast engagement.
– *Example 5:* Reports and informations on the local situation are often valuable to decision makers in a control center. This kind of policy can be used to harness mobile users as human sensors, i.e. requesting them to send in reports or digital photos that document local effects if a disaster. It thus implements a kind of query on human sensors.
– *Example 6:* In case that only the location addressing is used, a pure geo-casting functionality can be realized. This can for example be used to send out urgent warnings to all mobile users involved in a rescue mission.

8 Security Analysis

In the following, we assess the security provided by our proposed approach to end-to-end secure attribute-based messaging. Firstly, we discuss the novel hybrid encryption technique. Then, the fulfillment of the security requirements relevant to emergency communication (cf. Section 3.2) is investigated.

8.1 Discussion of Hybrid Encryption

The proposed design of the hybrid encryption technique follows two main goals: achieving efficiency in handling continuous dynamic attributes and minimizing trust requirements in attribute authorities at the same time. We recap our design decisions and discuss the resulting level of security.

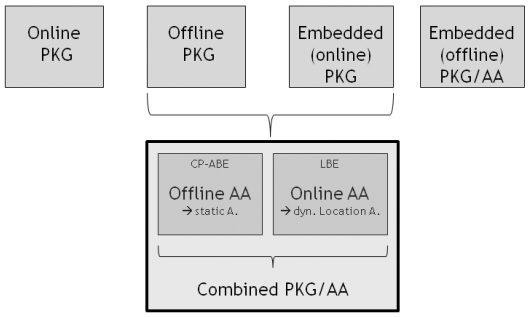

Fig. 16. Generation of private keys: design space and chosen approach

At first, handling dynamic attributes requires means for providing keys on mobile devices. An *online AA* (or online PKG) could principally solve the problem, but does not scale. An *offline AA* only allows handling dynamic attributes by pre-registering all possible attributes to a local trusted activator. This is inefficient for continuous attributes. An *embedded AA* could be implemented locally on tamper-resistant hardware. However, it locally requires the master key and could generate all attributes of all users, such that the key escrow risk associated to a compromise is extremely high. Within our approach, we propose to conceptually split the role of the single *AA* (cf. Figure 16): an *offline CP-ABE AA* issues all static attributes in a registration phase, while an *embedded LBE AA* handles dynamic location attributes, based on tamper-resistant hardware.

W.r.t. to encryption security, the hybrid technique is designed such that the loca-tion-based encryption (LBE) parts adds a further level of security to the symmetric session key that is used for message encryption. In our approach, the XOR operation encrypts the initially generated session key comparable to an one-time pad [28]. Hence, decryption is only possible if the required CP-ABE attributes are available to decrypt the outer asymmetric encryption layer and the location lock value can be generated correctly in order to recover the session key.

In most cases, messaging policies include a conjunction of location and further CP-ABE attributes (cf. Figure 15). Then, this approach retains encryption of messages even in case the *embedded LBE AA* is compromised.

Moreover, in case the CP-ABE attributes are compromised, a message is still protected by the additional location-dependent encryption layer. Thus, the hybrid encryption technique allows realizing end-to-end encryption while being able to handle expressive policies.

In addition, our proposal minimizes the use of pairings in the end-to-end encryption. This design broadens the applicability of the encryption technique to a range of mobile devices. In turn, the hybrid encryption technique looses full cryptographic collusion resistance w.r.t. the expressive policy. Yet, a collusion between receivers or adversaries that try trading CP-ABE attributes, e.g. in order to gain access to messages of further organizations, fails.

The hybrid encryption assumes tamper-resistant hardware, especially a tamper-resistant GPS receiver. In the emergency response application context, this assumption is practically fulfilled, e.g. by given TETRA mobile communication devices.

The application logic required to implement the location lock mapping and the location verification procedure is small, such that means to guarantee correctness based on certification procedures can easily be applied. Together with a secure software stack supported by a TPM chip of the mobile device [7], additional practical security guarantees could be given.

In some cases, a device may be unable to compute its current GPS position, e.g. inside closed buildings. To circumvent functional problems, we propose to internally rely on the last computed (and thus computable) GPS position in such cases.

8.2 Security Analysis of Mechanisms

In this section, we discuss the fulfillment of the security requirements relevant to emergency communication.

- `SReq1: Basic security:` The basic security mechanisms of mutual authentication, message integrity and availability are given by the security architecture of the emergency communication network (cf. 5.4). Since the ABM scheme is realized on the end-to-end encryption layer, they apply to it, too. Especially, device revocation is possible by means of the network, without relying on additional cryptographic mechanisms on the application level.
- `SReq2: End-to-end confidentiality w/o online PKG:` End-to-end encryption in the messaging is given due to and implemented by the use of the proposed hybrid encryption technique on the end-to-end encryption layer. In particular, the enforcement of the LBE part of expressive policies hinges on tamper-resistant GPS receivers. In addition, computational security reduces to the same computational assumptions as in CP-ABE. For more details, we refer to [2]. Collusion resistance is given as discussed in Section 8.1.
- `SReq3: Protection against replay attacks:` Replay attacks are handled on the end-to-end encryption layer: after decryption, the receiver verifies the freshness of the included message ID. The receiver rejects messages that contain an ID that she already decrypted. This mechanism requires that the message ID is unique due to its generation.
- `SReq4: Non-repudiation of senders:` Non-repudiation of senders is assured due to two mechanisms. Firstly, each message sent is added to the message log ML, for additional security digitally signed by the sender S. This record can later be analyzed. Secondly, each message includes a MAC, such that it can be linked to the sender, given that the registration information is correct.
- `SReq5: Documentation of readers:` Readers, i.e. the subset of all receivers of a message that satisfied the logical messaging policy, are documented via the readers list RL. In order to achieve this, readers have to send acknowledgements to the control center. The fulfillment of this requirement thus hinges on the compliance to the protocol for end-to-end secure attribute-based messaging (cf. Figure 14)[13]. Unique mobile subscriber identities, $IMSI_R$, can be resolved to real world identities of readers, by linking them to information present on the registration list $RegL$.
- `SReq6: Efficiency of security mechanisms:` Efficiency of the proposed ABM scheme has computational and organizational factors. Regarding computational efficiency, our approach has a low pairing complexity. Firsthand, this is achieved by the design of the messaging policies (cf. Figure 2) as well as by the proposed hybrid encryption mode. In particular, the session key decryption requires one XOR operation for the LBE part. In order to decrypt the CP-ABE part of the policy, two pairing operations for every

[13] For additional security, the software modules implementing the protocol can be certified by a trust provider.

attribute that is matched by one of a receiver's attributes are required[14]. Yet, messaging policies are designed such that at most 6 pairing operations are required. Thus, the hybrid policy encryption technique together with the policy design render the decryption practically in real time on resource-constrained devices (cf. [35]). From the organizational perspective, no online PKE is required, such that the number of interactions that are required for the end-to-end key management are reduced to a single registration phase.

- `SReq7: Appropriateness to users:` Appropriateness to users is supported by the following factors. Firstly, our ABM approach allows for a single, combined realization of all necessary communication patterns `CP1-CP4` (cf. Section 3.1). It thus minimizes learning efforts.
  Secondly, our approach integrates continuous location attributes into the selection of receivers, which are intuitive selectors for senders. Thirdly, more generally, the approach has been designed based on insights that were derived from experiments with potential real users. We discuss this issue more closely in Section 6.
- `SReq8: Receiver anonymity:` From the receivers' perspective, the given approach allows for an acceptable integration into personal lives, since privacy protection is given due to the following mechanisms. Firstly, every registered mobile user can be efficiently contacted and requested via an implicit addressing method that includes location. In particular, in our proposal this is possible without disclosing identifying information along with location updates beforehand. Instead, the implicit addressing is based on broadcasts and local enforcement (by means of the hybrid encryption technique) on the mobile device. This kind of privacy protection achieved by broadcast- and implicit addressing-based communication mechanisms is denoted receiver anonymity in the literature (cf. [20]).

In Table 1, we summarize the security requirements and the proposed security mechanisms. The fulfillment of protection goals reduces to cryptographic assumptions and trusted processes. Moreover, the implementation of functionalities for implicit addressing on mobile devices (which in turn require trusted hardware) is a key mechanism to achieve privacy protection. In addition, our design is also based on experiences with real users. This issue was discussed in more detail in the Section 6.

9 Conclusion

This paper dealt with security issues inherent to one-to-many communication with mobile and anonymous receivers. Throughout this article, we used the context of emergency communication as a descriptive application scenario. In order

[14] In case the approach would be extended to policies with additional internal AND-/OR-levels, one exponentiation operation would be required for each internal node from an attribute in the leaf to the root node of the CP-ABE policy part.

Requirement	Mechanisms
SReq1: Basic security	Mutual authentication Message integrity Availability Device revocation (all given by network)
SReq2: End-to-end confidentiality w/o online PKG	Hybrid encryption technique (based on offline and embedded PKG) (based on tamper-resistant GPS receiver) Collusion resistance (based on CP-ABE)
SReq3: Protection against replay attacks	Message ID (based on unique generation of IDs)
SReq4: Non-repudiation of senders	Message authentication codes (based on key distribution) Message log
SReq5: Documentation of readers	Acknowledgements (based on compliance to protocol) Message authentication codes (based on key distribution) Readers list (based on correct registration information)
SReq6: Efficiency of security mechanisms	Policy design Hybrid encryption mode (based on encryption technique) Offline key generation (based on registration)
SReq7: User -friendliness	Single communication mechanism Intuitive location selection Design tailored to end users (based on experiments)
SReq8: Receiver anonymity	Broadcast Implicit addressing (based on local enforcement on device)

Table 1. Security requirements and employed mechanisms

to devise an user-friendly yet secure communication support, we followed a participatory design approach. Based on experiences with emergency practioners, we jointly elicited security requirements and derived a design proposal. Then, we proposed a solution harnessing an attribute-based messaging approach. In particular, in order to meet end-to-end confidentiality needs, we conceptualized a hybrid encryption technique. Its application within an emergency communication network enables end-to-end secure yet user-friendly communication mechanism, that also takes into account receiver anonymity and non-repudiation.

We believe that ABM concepts have the potential to become an important communication paradigm in mobile and pervasive computing scenarios, due to the inherent user-friendliness, practicality and flexibility. Further user trials in different application domains can help to understand how a large range of casuals users prefer to interact with and by an attribute-based messaging system, in order to develop its full potential.

References

1. Al-Fuqaha, A., Al-Ibrahim, O.: Geo-Encryption Protocol for Mobile Networks. Computer Communications 30(11-12), 2510–2517 (2007)
2. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy. pp. 321–334. IEEE CS (2007)
3. Blackmon, M.H.: Cognitive Walkthrough. In: Bainbridge, W.S. (ed.) Encyclopedia of Human-Computer Interaction - Volume 1, pp. 104–107. Berkshire Publishing Group (2004)
4. Bobba, R., Fatemieh, O., Khan, F., Gunter, C.A., Khurana, H.: Using Attribute-Based Access Control to Enable Attribute-Based Messaging. In: Annual Computer Security Applications Conference (ACSAC '06). pp. 403–413. IEEE CS (2006)
5. Bobba, R., Fatemieh, O., Khan, F., Khan, A., Gunter, C.A., Khurana, H., Manoj, P.: Attribute-Based Messaging: Access Control and Confidentiality. ACM Transactions on Information Systems Security (TISSEC) 13, 31:1–31:35 (December 2010)
6. Boneh, D., Franklin, M.K.: Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing 32(3), 586–615 (2003)
7. Brucker, A.D., Petritsch, H., Weber, S.G.: Attribute-Based Encryption with Break-Glass. In: Workshop on Information Security Theory and Practice (WISTP'10). pp. 237–244. Springer (2010)
8. Chadwick, D., Lunt, G., Zhao, G.: Secure Role Based Messaging. In: IFIP Conference on Communications and Multimedia Security (CMS '04). pp. 303–316 (2004)
9. Committee on Planning for Catastrophe (ed.): Successful Response Starts With A Map: Improving Geospatial Support for Disaster Management. National Academy Press (2007)
10. Denning, D.E., Scott, L.: Geo-Encryption - Using GPS to Enhance Data Security. GPS World (2003)
11. Flentge, F., Weber, S.G., Behring, A., Ziegert, T.: Designing Context-Aware HCI for Collaborative Emergency Management. In: Int'l Workshop on HCI for Emergencies in conjunction with CHI '08 (2008)
12. Gentry, C.: IBE (Identity-Based Encryption). In: Bidgoli, H. (ed.) Handbook of Information Security - Volume 2, pp. 575–592. John Wiley and Sons (2006)

13. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In: ACM Conference on Computer and Communications Security (CCS '06). pp. 89–98. ACM Press (2006)
14. Karabulut, Y., Weppner, H., Nassi, I., Nagarajan, A., Shroff, Y., Dubey, N., Shields, T.: End-to-End Confidentiality for a Message Warehousing Service using Identity-Based Encryption. In: ICDE Workshops. pp. 33–40 (2010)
15. Linde, C.: Aufbau und Technik des digitalen BOS-Funks. Franzis Verlag (2008)
16. Martin, L.: Identity-Based Encryption: A Closer Look. ISSA (Sep.), 22–24 (2005)
17. Maurer, U.M.: Modelling a Public-Key Infrastructure. In: European Symposium on Research in Computer Security (ESORICS '96). pp. 325–350. Springer (1996)
18. Mont, M.C., Bramhall, P., Harrison, K.: A Flexible Role-Based Secure Messaging Service: Exploiting IBE Technology for Privacy in Health Care. In: Workshop on Database and Expert Systems Applications (DEXA '03). pp. 432–437. IEEE CS (2003)
19. Murgatroyd, B.W.: End to End Encryption in Public Safety TETRA Networks. IE Seminar on Secure GSM and Beyond: End to End Security for mobile Communication (Digest No. 2003/10059) (2003)
20. Pfitzmann, A., Waidner, M.: Networks without User Observability. Computers and Security 6, 158–166 (May 1987)
21. Pfitzmann, A., Juschka, A., Stande, A.K., Steinbrecher, S., Köpsell, S.: Communication Privacy. In: Digital Privacy: Theory, Technologies and Practices, pp. 19–45. Taylor & Frances (2007)
22. Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure Attribute-Based Systems. In: ACM Conference on Computer and Communications Security (CCS '06). pp. 99–112. ACM Press (2006)
23. Rannenberg, K.: Multilateral Security - a Concept and Examples for Balanced Security. In: Workshop on New Security Paradigms (NSPW '00). ACM Press (2000)
24. Sahai, A., Waters, B.: Fuzzy Identity-Based Encryption. In: Advances in Cryptology - EUROCRYPT '05. pp. 457–473. Springer (2005)
25. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-Based Access Control Models. IEEE Computer 29(2), 38–47 (1996)
26. Scott, L., Denning, D.E.: A Location Based Encryption Technique and Some of Its Applications. In: ION National Technical Meeting 2003. pp. 730–740 (2003)
27. Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612–613 (1979)
28. Shannon, C.E.: Communication Theory of Secrecy Systems. The Bell System Technical Journal 28, 656–715 (1949)
29. Tognazzini, B.: Design for Usability. In: Cranor, L., Garfinkel, S. (eds.) Security and Usability: Designing Secure Systems That People Can Use, pp. 31–96. O'Reilly Media (2005)
30. Turoff, M., Chumer, M., Van de Walle, B., Yao, X.: The Design of a Dynamic Emergency Response Management Information System (dermis). The Journal of Information Technology Theory and Application (JITTA) 5(4), 1–35 (2004)
31. Weber, S.G.: Harnessing Pseudonyms with Implicit Attributes for Privacy-Respecting Mission Log Analysis. In: Conference on Intelligent Networking and Collaborative Systems (INCoS '09). pp. 119 – 126. IEEE CS (2009)
32. Weber, S.G.: Secure and Efficient First Response Coordination Based on Attribute-Based Encryption Techniques. ISCRAM '09 Poster Session (2009)
33. Weber, S.G.: Securing First Response Coordination with Dynamic Attribute-Based Encryption. In: Conference on Privacy, Security and Trust (PST '09) in conjunction

with World Congress on Privacy, Security, Trust and the Management of e-Business (CONGRESS '09). pp. 58 – 69. IEEE CS (2009)
34. Weber, S.G.: A Hybrid Attribute-Based Encryption Technique Supporting Expressive Policies and Dynamic Attributes. Information Security Journal: A Global Perspective 21(6), 297–305 (2012)
35. Weber, S.G.: Multilaterally Secure Pervasive Cooperation - Privacy Protection, Accountability and Secure Communication for the Age of Pervasive Computing. IOS Press (2012)
36. Weber, S.G., Kalev, Y., Ries, S., Mühlhäuser, M.: MundoMessage: Enabling Trustworthy Ubiquitous Emergency Communication. In: International Conference on Ubiquitous Information Management and Communication (ICUIMC '11). pp. 29:1–29:10. ACM Press (2011)
37. Weber, S.G., Mühlhäuser, M.: Multilaterally Secure Ubiquitous Auditing. In: Intelligent Networking and Collaborative Systems and Applications, SCI 329, pp. 207–233. Springer (2010)
38. Yuan, E., Tong, J.: Attribute Based Access Control (ABAC) for Web Services. In: Conference on Web Services (ICWS'05). pp. 561 – 569. IEEE CS (2005)