Towards Trustworthy Identity and Access Management for the Future Internet

Stefan G. Weber, Leonardo A. Martucci, Sebastian Ries and Max Mühlhäuser
Telecooperation Group, Technische Universität Darmstadt and
Center for Advanced Security Research Darmstadt (CASED)
Mornewegstr. 32, DE 64293, Darmstadt, Germany
{*firstname.lastname*}*@cased.de*

***Abstract*—The Future Internet, in its different variants, promises a global connectivity of people, things and services. However, in order to develop its full potential and to achieve an accepted, seamless integration of Internet use into daily lives, severe security issues have to be addressed. In this paper, we propose to establish security and trustworthiness by means of an integrated identity and access management. Especially, we sketch the foundations of a novel identity and access management approach that is tailored for the Future Internet. We provide mechanisms for flexible modeling and description of digital user identities with support to transaction-based privacy protection, access to personal data, flexible third-party accountability and end-to-end secure communication. The mechanisms are tailored for the use on a trusted personal device called Minimal Entity, which provides a trustworthy gateway to benefit from the offerings of the Future Internet.**

***Keywords- identity and access management*; *security*; *privacy*; *Future Internet*.**

I. Introduction

The Internet of People, Things, and Services are three fundamental concepts that form the backbone of the Future Internet [1]. The Internet of Things (IoT) relates to interconnected physical devices, usually in the form of embedded systems and sensors with one or more network interfaces that are used to collect, forward, compute, or display data. The objective of the Internet of Services (IoS) is to set up a fully-fledged digital equivalent of the existing service-based economy. Thus, IoS allows people and software-based entities to engage in service-based economic activities, such as negotiation, bidding, and contracting. Moreover, the interweaving of simple services into complex and efficient composite services through the IoS will turn it into the global marketplace of the future. The Internet of People (IoP) relates to human-machine interfaces that allow people to interact within the Future Internet. The IoP basically empowers users with service-independent ubiquitous access. Together the Internet of People, Things and Services are known by the acronym IoPTS.

Two further concepts associated with the Future Internet are the Internet of Clouds and Crowds [1]. They are a platform and, respectively, a facilitator for boosting the IoPTS. The Internet of Clouds provides (low-end) devices with extended computing and storage services, that otherwise would not be available using only local resources. In addition, the Internet of Clouds adds elasticity, reliability and cost-effectiveness to service provision. The Internet of Crowds brings the benefits of social networks into the IoPTS. It establishes valuable connections harnessing social interactions and other tools based on those, such as trust and reputation mechanisms.

The assessment of trust and reputation within IoPTS contexts and the proliferation of trustworthy services for end users require the definition of common metrics. Metrics are fundamental for defining a uniform and coherent set of service-level agreements (SLAs), that allow a fair competition between services providers, thus fostering innovation and the introduction of new services. Furthermore, common metrics also allow the interoperability between services and communication platforms, which are key aspects in the IoPTS.

The realization of the IoPTS in a global scale ultimately depends on a provider-independent ubiquitous access of casual users to the Future Internet. Ubiquitous access together with intuitive interfaces and interaction concepts that support enforcement of users' wishes and needs have to be offered independently of any service or communication provider. In this context, our research group has been developing and constantly refining the notion and concept of the *Minimal Entity* (ME) as the users's personal connection point and trustworthy gateway to the IoPTS and implemented a ME prototype, the so-called Talking Assistant [2]–[4].

In short, the ME is a user's representative in the digital world. It stores a user's digital identity and is able to perform operations such as remote authentication. The ME is designed as a secure terminal and thus enables secure transactions, possibly with legal impact. We propose that the interaction between users and IoPTS is going to happen through personal devices, thus such devices can work as anchors of trust. In some cases, the ME may even carry out transactions with only implicit consent of the user, depending on the application context. Hence, it is of utter importance for the success of IoPTS that a user trusts the ME to execute tasks trustworthy and independently of user interventions.

In this paper, we continue this line of work and introduce a comprehensive digital identity and access management (IAM)[1] approach for MEs, tailored for the IoPTS. By this, we introduce concepts and trust anchors that enable:

- transaction-based privacy protection,
- provider-independent access to transaction data,
- flexible third-party accountability, and
- user-friendly, end-to-end secure communication.

The objective of this paper is to propose security and privacy-enhancing mechanisms suitable to emergent trustworthy ubiquitous cooperation and interactions in the IoPTS. Such interactions are obtained by interconnecting multiple parties, entities and services, in the face of possibly conflicting individual security goals [5]–[7]. The Future Internet, represented by the interwoven IoPTS variants, provides the service-provisioning infrastructure and data communication backbone for our vision to come true.

In the remaining of this section, we summarize the contributions of our work in Section I-A and outline the structure of this paper in Section I-B.

A. Our Contributions

In this paper, we propose a novel IAM approach that is tailored to foster cooperation in the Future Internet. The approach builds on a carefully chosen combination of modern cryptographic techniques for modeling and implementing the core identity abstractions and corresponding security services.

Our solution takes into account and deals with the conflicting requirements of privacy and accountability. Privacy requires a restricted linkability between users and actions, while accountability demands strong and irrefutable linkability between users and performed transactions. In this context, a novel pseudonym construction is a key building block to our IAM approach. It protects users' privacy and provides accountability simultaneously. Moreover, our proposal includes mechanisms for end-to-end secure communication within anonymous groups and also fosters incentives for trustworthy cooperation through being compatible with reputation mechanisms.

B. Paper Structure

This paper is organized as follows. Section II provides a more detailed description of the research challenges of this paper. An application scenario for the proposed model is described in Section III. The attacker model is presented in Section IV. The system requirements are outlined in Section V. Section VI describes our novel IAM system designed for the Future Internet. The discussion regarding the security and privacy properties of the proposed concept in the light of the attacker model is described in Section VII. Section VIII presents the related work. Finally, the concluding remarks are given in Section IX.

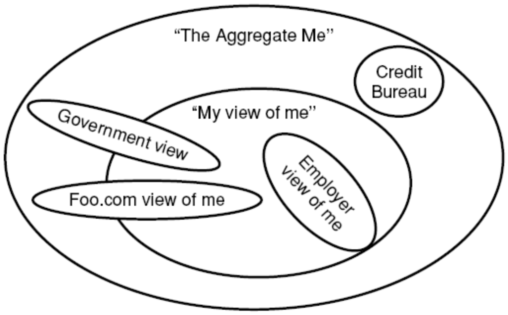

Figure 1. Multiple Views of a Digital Identity [8].

II. Towards Trustworthy IAM

The notion of identity and access management (IAM) encompasses a broad range of techniques, technologies and processes that support the use of real world properties of real world entities as digital identifiers in computer networks and applications [8]. Herein, a *digital identity* abstracts from a real world person, implementing a unique digital representation of the entity. Also, this profile details relationships to other entities or parties and contains associated access rights and credentials [9].

Due to the use in different application contexts, different interaction partners may build up different, possibly restricted, views of a complete identity, by aggregating data collected in multiple individual interactions (cf. Fig. 1). This reflects major challenges of IAM:

- how to flexibly model digital identities?
- how to provide support for trustworthy digital interactions with different parties?
- how can aggregation be limited in order to protect users' privacy?

The next sections develop a more concrete understanding of trustworthy and secure interactions in the Future Internet.

III. Application Scenario

In our application scenario, we consider a Web 2.0 running on top of the IoPTS. Thus, we deal with a collaborative environment where users provide content to a common pool of digital resources and recommend reading material and links to their community.

To protect users' privacy, digital content and recommendations are provided using identifiers that are not the users' real names. Naturally, such capabilities can be exploited by malicious users who could provide misleading information, badmouth other users, or even commit an infringement of the law. Therefore, such misbehaving users need to identifiable by trusted authorities.

[1] In this paper, we treat IAM as a synonym to Identity Management (IdM). However, we use IAM to emphasize the inherent access control issues that are related to digital identities in the IoPTS.

In this paper, we consider such a scenario. First, we show how to create linkable, thus accountable pseudonyms. Then, we demonstrate how the identity of a malicious user can be retrieved by authorities. Furthermore, we also show how secure communication can be performed within such a representative IoPTS scenario.

IV. Attacker Model

In this paper we consider a limited version of the Dolev-Yao threat model [10]. In the Dolev-Yao threat model the attacker has control of all communication channels, being able to eavesdrop messages in transit, destroy, replay and insert messages into these channels. However, the attacker is not able to break any cryptographic mechanisms without obtaining the appropriate cryptographic keys (i.e., attackers do not have cryptanalysis capabilities).

In our paper we restrict the Dolev-Yao model by removing the ability of attackers to destroy messages in transit indiscriminately. The deletion of messages in transit in a computer network scenario leads to denial of service attacks. Although such type of attacks are physically plausible in real scenarios (but mostly limited to a local scope) using radio jamming techniques, we disregard such attacks because they are not the focus of our proposed IAM system.

V. Requirements for Trustworthy IAM

Based on the application scenario and the attacker model, in this section, we introduce a set of requirements for an IAM approach suitable for the IoPTS:

- *Network-Level Basic Security Services:* The network should provide identification, mutual authentication, reliable broadcast communication and user revocation.
- *Privacy I:* Identity-related information should be protected in transactions.
- *Privacy II:* It should be possible to individually access data that relates to personal transactions.
- *Accountability:* It should be possible to trace misbehaving users (by accredited authorities).
- *Secure Communication I:* End-to-end confidential communication between entities should be possible.
- *Secure Communication II:* It should be possible to communicate with receivers unknown by identity.
- *Incentives:* The mechanisms should be incentive compatible, e.g. support the use of social reputation mechanisms.
- *Efficiency and Practicality:* Trust anchors and mechanisms should be suitable for use on resource-constrained terminal devices and in real-world contexts.
- *User-Friendliness:* Security concepts should be understandable and usable by casual users.

The main factors are also illustrated in Fig. 2.

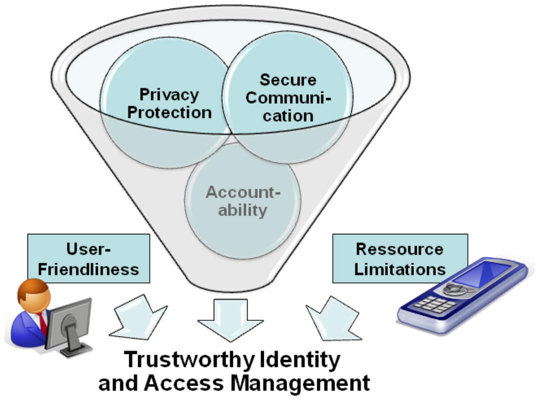

Figure 2. Main Factors for IAM

VI. Model

In this section, we sketch our novel approach to identity and access management for the Future Internet. First, we introduce our key concepts that lead to a set of core functional identity abstractions. Then, we depict mechanisms and technical details implementing our IAM approach.

A. Network Model

We assume the following network model as depicted in Fig. 3 to be given by the Future Internet: each user is in possession of a personal terminal device, called minimal entity (ME). By means of the terminal, a user can securely log in to the network and communicate in broadcast-style. The network access can be revoked. Application level security services are enabled through certain credentials, that the user receives in a prior registration process, dependent on his real world properties. Together, the credentials represent the user's digital identity. We detail this issue next.

B. Key Concepts

The IAM approach builds upon two main concepts:

1) Enabling privacy-respecting yet accountable transactions through linkable pseudonyms: First, we base our IAM design on the use of linkable transaction pseudonyms, i.e. pseudonym that change with every single transaction. We propose to embed access rights for multiple parties

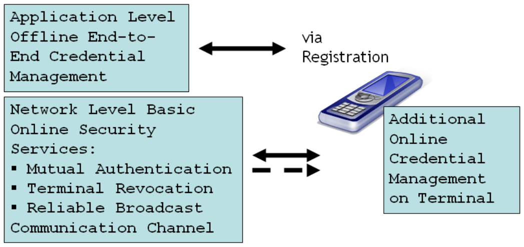
Application Level Offline End-to-End Credential Management
via Registration
Network Level Basic Online Security Services:
▪ Mutual Authentication
▪ Terminal Revocation
▪ Reliable Broadcast Communication Channel
Additional Online Credential Management on Terminal

Figure 3. Network Model

into each pseudonym, that allow accredited authorities to link the pseudonyms to the implicit identity in several levels granularity. In this concept, transaction pseudonyms implement privacy protection, while the given multilevel, multiparty linkability allows to deal with accountability issues by enabling a purpose-bound anonymity revocation, e.g. in misuse cases [11].

2) Leveraging fuzzy cryptographic identities on trusted devices for user-friendly communication: Second, we propose to describe static aspects of identities as sets of attributes that relate to sets of key [12]. Attributes in logical combination can be used to intuitively select receivers in end-to-end secure communication [13], [14]. Additionally, in our security design, we harness a Trusted Platform Module (TPM) in the terminal device to locally generate and use context-dependent credentials and attributes, that may be exploited in the receiver addressing as well.

C. Core Identity Abstractions

In sum, the two main concepts introduced above are reflected in the following core identity abstractions. Thus, from a conceptual point of view, a digital identity, as depicted in figure 4, consists of the following properties, organized into three layers:

I. one unique base identifier, i.e. the real world name in the respective domain (e.g. "StefanGWeber@Darmstadt");

II. static properties, i.e. organizational and economical roles (e.g. "CASED") and attributes used in social digital interactions and communications (e.g. specializations, preferences or interests);

III. dynamic properties, i.e. context-dependent, dynamic attributes (e.g. current location of the user).

Each conceptual layer is associated with keying material in order to implement security functionalities, i.e. privacy protection, accountability management and support for confidential communication. A minimal entity, i.e. a personal terminal device, provides the digital container, platform and trust anchor for this approach. We introduce the mechanisms in the following sections.

D. Main Mechanisms

In the following, we sketch[2] the constructions and mechanisms of our approach:

1) Creation of Transaction Pseudonyms via Semantically Secure Encryption: We propose to generate changeable pseudonyms by means of a semantically secure encryption scheme (cp. [11], [15], [16]). Thus, we formulate pseudonym creation as (re-)encryption of a base identifier. Using this approach, it is possible to change a transaction pseudonym represented by a ciphertext, without changing the encrypted plaintext and without private key, by just altering the random factors used in the encryption.

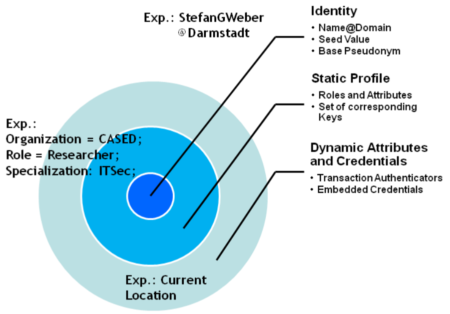

Figure 4. Layers of IAM

Especially, we propose to employ the ElGamal cryptosystem [17], over subgroups $\mathbb{G}_q$ of order q of the multiplicative group $\mathbb{Z}_p^*$, for large primes $p = 2q + 1$. We treat the primes p, q and a primitive element g of $\mathbb{G}_q$ as common system parameters. More specifically, we build upon a threshold variant of it [18], [19], offering distributability of powers. In this setting, an ElGamal private key $s \in_R \mathbb{Z}_q$ is generated via a distributed key generation protocol [18], and consequently it is secret shared [20] among all n participating authorities. Thus, the power to decrypt is distributed among all authorities, while a minimal number of t out n authorities is necessary to perform the private key-related operations. The authorities share a common public key, $h = g^s \bmod p$, that is made available together with the system parameters. In our approach, a base pseudonym $P_{U_i,B}$ of a user U_i is initially created as encryption of a representation of the base identifier ID. Thus, $ID \in \mathbb{G}_q$ is non-deterministically encrypted by choosing $r \in_R \mathbb{Z}_q$ and by computing $(g^r, h^r ID)$. Afterwards, transaction pseudonyms can be derived from the base pseudonym by iterative re-encryption (where $k \in \mathbb{N}$ refers to the k^{th} transaction and $\otimes$ denotes multiplication): $P_{U_i,k+1} = P_{U_i,k} \otimes g^{r_{k+1}} = (g^{r+r_{k+1}}, h^{r+r_{k+1}} ID)$

2) Achieving Pseudonym Linkability through PRNGs and SMPC: Due to the construction given above, a transaction pseudonym is initially statistically unlinkable to any other transaction pseudonym of any user. However, we introduce a further level of control into pseudonym generation by means of a local cryptographically-secure pseudo-random number generator (PRNG) [21]. Such a PRNG is a tool for generating sequences of random numbers, by using an internal source of entropy called seed to derive the output values. Only the owner of the seed is able to (re-)generate the chain of random numbers. We use a seeded PRNG to compute the re-encryption factors in the pseudonym generation. By this, each re-encryption factor becomes (part of) a unique authenticator for a transaction pseudonym. Given that all transaction data in a Future Internet service is stored along with a transaction pseudonym, a provider-

[2] Complete descriptions will be given in a longer version of this paper.

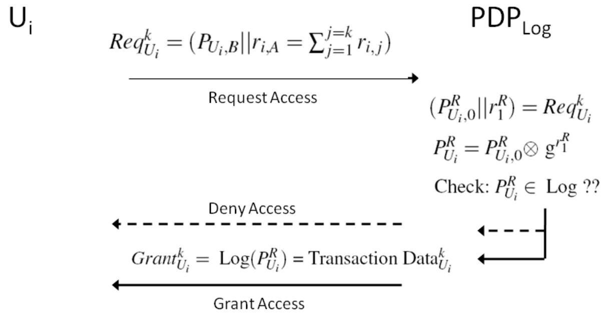
$\mathrm{U_i}$
$\mathrm{PDP_{Log}}$
$Req^k_{U_i} = (P_{U_i,B} || r_{i,A} = \sum_{j=1}^{j=k} r_{i,j})$
Request Access
$(P^R_{U_i,0} || r^R_1) = Req^k_{U_i}$
$P^R_{U_i} = P^R_{U_i,0} \otimes \mathrm{g}^{r^R_1}$
Check: $P^R_{U_i} \in$ Log ??
Deny Access
$Grant^k_{U_i} =$ Log$(P^R_{U_i})$ = Transaction Data$^k_{U_i}$
Grant Access

Figure 5. Protocol for Access to Transaction Data

independent access mechanism to personal transaction data can be implemented as follows: by providing the base pseudonym together with aggregated random factors, a user can uniquely authenticate any transaction pseudonym that was created by her; upon verification, the provider may grant access to associated transcation data to the requesting user. The basic access protocol is depicted in Fig. 5 (PDP_{Log} denotes the policy decision point of the service provider's transaction log and || denotes a separator for the parts of a tuple).

Additionally, our approach employs secure multiparty computation (SMPC) concepts [22] in order to realize multilevel pseudonym linkability. This allows for re-identifying a pseudonym in arbitrary levels of granularity. Herein, our constructions make use of mix-and-match techniques [11], [16], [19][3]. Especially, in this approach, several parties have to cooperate in order to partially revoke pseudonymity for accountability reasons in a given application context. The roles of the authorities could be played by established auditors, data protection officers as well as law enforcement authorities, in severe misuse cases.

3) Using Linkability for Reputation Aggregation: Within our approach, it is also possible to connect privacy-protection via transaction pseudonyms with reputation mechanisms. Through reputation mechanisms, users are supported to select reputable interaction partners, based on aggregated historical trust and reputation values and recommendations [23]. In order to compute reputation scores, it is necessary to establish interaction histories, i.e. aggregating experiences over past transactions. Again, due to the applicability of SMPC techniques on the pseudonym level, interaction histories can be established as follows: suppose that $RA_1, ..., RA_n$ are a set of reputation aggregation authorities, assessing pseudonym - value tuples, $(P_1, V_1), ..., (P_n, V_n)$, as inputs. The pseudonym linkability/mix-and-match framework enables them to compute a function $f((P_1, V_1), ..., (P_n, V_m)) = X$, whereby X can assert identity linkability information as well as an aggregated reputation score or update value. Moreover, correctness of the output and privacy of the inputs can be guaranteed [22], without relying on a single, external trusted party.

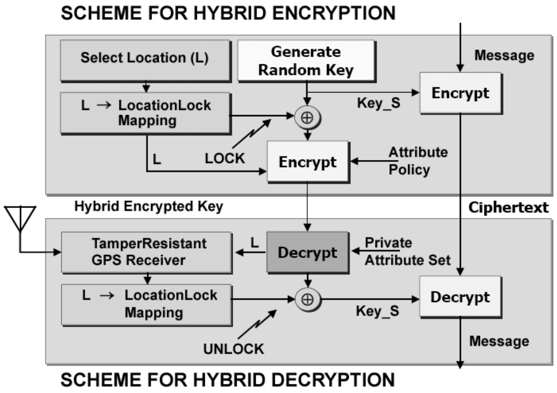

Figure 6. Hybrid Encryption Technique for Expressive Policies

4) End-to-End Secure Communication with Anonymous Receivers through Expressive Encryption: We propose to realize the attributes and credentials associated with a digital identity's static profile through ciphertext policy attribute-based encryption (CP-ABE) techniques [24]. Dynamic, context-dependent credentials are handled by means of generalized location-based encryption [25]. By combining these two approaches efficiently, we realize a novel hybrid encryption technique for expressive policies (cf. Fig. 6) [14].

This integrated approach allows to realize a secure group communication mechanism (w.r.t. to the specified network model, cf. Sec. VI-A) with an intuitive selection of communication partners. As sketched in Fig. 7, a user may send messages to groups of users specified by a logical combination of several attributes. We believe that this is an adequade approach for social communication contexts emerging in the Internet of People, where communication partners are often not known by identity, but only by property.

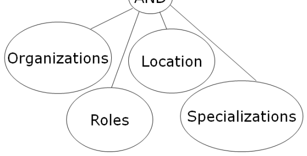

Figure 7. User-Friendly Selection of Communication Partners

[3] Details are beyond the scope of this, we only point to the literature.

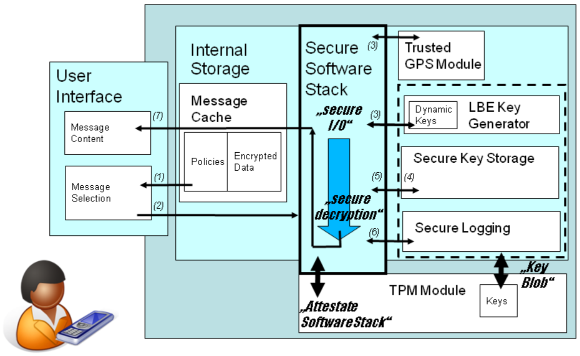

Figure 8. TPM-Based Attribute Handling on Terminal

E. Minimal Entity Security Design

In this section, we sketch issues related to the security design of the terminal device, i.e. the Minimal Entity.

In our approach, the hybrid encryption technique for secure communication hinges on a tamper-resistant GPS receiver. It triggers the creation of keys that need to satisfy location-depended constraints in the communication. We propose a security infrastructure that is based on trusted platform modules (TPM) in the terminal device. It is sketched in Fig. 8, illustrating the logical protocol for decryption of a received/chosen message. Herein, the TPM attestates that the software stack is trusted, such that keys provided for decryption are only used when appropriate and erased consecutively [26].

In our research, we evaluated the design space of key and credential management procedures. Basically, private key and credential generation (PKG) is possible online, offline and embedded in tamper-resistant hardware. With the proposed combination (see Fig. 9) within our security design, we chose to move a major part of trust into the organizational level: attributes and keys are only issued in a trustworthy registration process. On the other hand, we move the trust for handling context-dependent credentials into the terminal device, and secure it by means of a TPM.

F. Overview of Phases and Participants

Having sketched the main mechanisms of our novel IAM approach, Fig. 10 finally provides an overview of the sketched processes for identity and access management.

VII. Security Discussion

In our attacker model (cf. Sec. IV), we assumed that a general attacker in the IoPTS is able to eavesdrop any messages transmitted, but cannot destroy messages as well as break cryptography. In this section, we sum up the key arguments w.r.t. the fulfillment of the addressed security requirements, in the light of this attacker model, where appropriate:

- *Privacy and Accountability:* Identity-related information is protected due to the use of transaction pseudonyms. ElGamal encryption, the main pseudonym building block, is semantically secure under the Decision Diffie-Hellman complexity assumption [27]. Thus, pseudonyms do not leak any partial information about the encoded base identity information to any attacker, who is not in possession of the private key. The allowed linking of several transaction pseudonyms for accountability reasons makes use of the mix-and-match/SMPC framework. Herein, security is also reduced to the same complexity assumption [19]. Stemming from operations of a threshold cryptosystem, powers to link pseudonyms are distributed among cooperating authorities, implementing a distribution of powers. Additionally, an operational separation of duty is given due to distinct authorities in distinct phases. Moreover, via the registration phase, we move trust into an organizational level.
- *Secure Communication:* End-to-end encryption in the messaging is given due to and implemented by the use of the proposed hybrid encryption technique. Computational security reduces to the same complexity assumptions as in CP-ABE [24]. In CP-ABE, collusion resistance[4], is given due to the use of individual random factors per user. The hybrid encryption technique looses full cryptographic collusion resistance w.r.t. the expressive policy. Yet, collusion between receivers or attackers that try trading CP-ABE attributes, e.g. in order to gain access to messages of further organizations, fails. Due to the tamper-resistant GPS receiver in combination with the secure software stack on the ME, trading of location attributes is also hindered.
- *Efficiency and Practicality:* In our security design, we chose a combination of trusted platform modules, trust-

[4] Since private keys are generalized into sets of attributes, the possibility of user collusions, i.e. combining attributes to generate a more powerful decryption key, must be excluded.

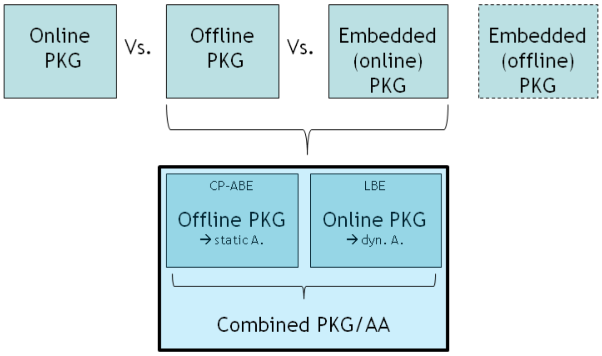

Figure 9. Design Space and Chosen Key Management Approach

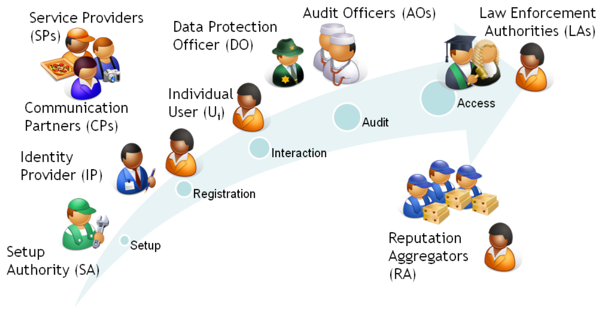

Figure 10. Overview

worthy registration processes as well as cryptographic complexity assumptions as trust anchors. TPMs become more and more common, even in mobile contexts, such that it is reasonable to assume their availability. Attribute-based encryption is the most ressource-demanding building block in our approach. Yet, our IAM-ME prototype implementation, based on off-the-shelf smartphones, showed reasonable performance[5]. Trustworthy registration processes are already by now established, e.g. for online banking, making their realizability reasonable.

- *User-Friendliness:* As part of our research, we confronted casual users with the proposed concepts for secure communication. Results indicated high levels of user acceptance and contributed to refining them[6].

VIII. Related Work

The related work can be clustered into the areas of linkable pseudonyms, secure attribute-based communication, as well as identity and access management approaches.

A. Linkable Pseudonyms

Historically, Chaum [28] introduced digital pseudonyms as a basic tool for privacy protection in distributed systems, by implementing a firsthand unlinkability between a real-world identity and a pseudonymized identity. In the following years, several types of pseudonyms and a wide scope of scientific background and applications has evolved [29]. Linkable pseudonyms are pseudonyms that additionally encode secret trapdoor information, to enable attribution of multiple pseudonyms to one or more real-world identities. Different from our work, linkability is usually only possible for either third parties or the user herself, not for both. Recent cryptographic research abstracts from pseudonyms and focuses on separating authentication from identification issues [30], but also allows for a reconciliation thereof, to construct so-called self-certified pseudonyms [31].

B. Secure Attribute-based Communication

Our work follows previous work on ABE [12], [24], [32] (in particular we extend the CP-ABE construction of [24]) and applications thereof [33], [34]. In this paper, we propose a novel use of attribute-based cryptography in the context of IAM.

C. Identity and Access Management

IAM is the target of initiatives such as Microsoft's Windows Cardspace[7] and OpenID[8]. The main focus of the aforementioned initiatives is related to the processes of creating, managing, and deleting identities. Research projects such as PRIME[9] and PrimeLife[10] address the problem of users' privacy in identity management systems in various application contexts. However, there is only little work done so far considering identity management and the trade-off between privacy and reputation establishment. Like our approach, the PRIME project recognized the need to reflect user-friendliness in the system design [35]. In [36], further aspects of IAM for the Future Internet are sketched, however, no technical approaches are presented.

IX. Conclusions

In this paper, we introduced and sketched a novel approach to identity and access management for the Future Internet. Hereby, we extended our former work on the concept of a Minimal Entity, i.e. a trusted personal terminal device that serves as gateway to the Future Internet. Our novel approach supports to reconcile transaction-based privacy protection and accountability via linkable pseudonyms as well as user-friendly end-to-end secure communication. The description and modeling of digital identities is based on a fruitful combination of modern cryptographic techniques. First, the use of semantically secure encryption techniques allows for the creation of changeable transaction pseudonyms. Harnessing mix-and-match techniques and PRNGs, we realize several levels of pseudonym linkability.

In sum, this constitutes a flexible framework for distribution of powers w.r.t. accountability measures as well as provider-independent fine-grained access to transaction-related information.

As a second major part, we harness attribute-based cryptography to describe and model user properties in combination with location-based encryption techniques on trusted personal devices. This enables end-to-end encrypted group communication, on an user-friendly high level of abstraction. Future work will consist of extensive resource and usability evaluations.

[5] A distinct performance evaluation will be part of a more complete version of this paper.

[6] A distinct evaluation of this issue will be part of a more complete version of this paper.

[7] (http://windows.microsoft.com/en-US/windows-vista/Windows-CardSpace)

[8] (http://www.openid.net)

[9] (https://www.prime-project.eu)

[10] (http://www.primelife.eu)

Acknowledgments

This work was supported by CASED (www.cased.de). The authors are responsible for the content of this publication.

References

[1] E. Aitenbichler, A. Behring, D. Bradler, M. Hartmann, L. Martucci, M. Mühlhäuser, S. Ries, D. Schnelle-Walka, D. Schreiber, J. Steimle, and T. Strufe, "Shaping the Future Internet," in *Proceedings of the 3rd International CompanionAble Workshop IoPTS*, 2009.

[2] E. Aitenbichler and M. Mühlhäuser, "The Talking Assistant Headset: A Novel Terminal for Ubiquitous Computing," Fachbereich Informatik, TU Darmstadt, Tech. Rep. Telecooperation Report No. 2, 2002.

[3] E. Aitenbichler, J. Kangasharju, and M. Mühlhäuser, "Talking Assistant: A Smart Digital Identity for Ubiquitous Computing," in *Advances in Pervasive Computing*. OCG, 2004, pp. 279–284.

[4] E. Aitenbichler and A. Heinemann, "Proximity-Based Authentication for Windows Domains," in *UbiComp 2007 Workshop Proceedings*, 2007, pp. 475–480.

[5] S. G. Weber, S. Ries, and A. Heinemann, "Inherent Tradeoffs in Ubiquitous Computing Services," in *INFORMATIK 2007*. GI, 2007, pp. 364–368.

[6] C. Patrikakis, P. Karamolegkos, A. Voulodimos, M. H. A. Wahab, N. S. A. M. Taujuddin, C. Hanif, L. Pareschi, D. Riboni, S. G. Weber, A. Heinemann, S.-C. S. Cheung, J. Chaudhari, and J. K. Paruchuri, "Security and Privacy in Pervasive Computing," *IEEE Pervasive Computing*, vol. 6, no. 4, pp. 73–75, 2007.

[7] S. G. Weber, A. Heinemann, and M. Mühlhäuser, "Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments," in *Workshop on Privacy and Assurance (WPA-2008)*. IEEE CS, 2008, pp. 958–964.

[8] J. Pato, "Identity Management," in *Encyclopedia of Cryptography and Security*. Springer, 2005, pp. 282–285.

[9] P. Windley, Ed., *Digital Identity*. OReilly, 2005.

[10] D. Dolev and A. C. Yao, "On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, Mar 1983.

[11] S. G. Weber and M. Mühlhäuser, "Multilaterally Secure Ubiquitous Auditing," in *Intelligent Networking and Collaborative Systems and Applications, Studies in Computational Intelligence, Vol. 329*. Springer, 2010.

[12] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *EUROCRYPT '05*. Springer, 2005, pp. 457–473.

[13] S. G. Weber, "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)*. IEEE CS, 2009, pp. 58 – 69.

[14] S. G. Weber, S. Ries, and M. Mühlhäuser, "Concepts and Scheme for Multilaterally Secure, User-Friendly Attribute-Based Messaging," in *submission*.

[15] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," in *Financial Cryptography*. Springer, 2003, pp. 103–121.

[16] S. G. Weber, "Harnessing Pseudonyms with Implicit Attributes for Privacy-Respecting Mission Log Analysis," in *Conference on Intelligent Networking and Collaborative Systems (INCoS 2009)*. IEEE CS, 2009, pp. 119 – 126.

[17] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[18] T. P. Pedersen, "A Threshold Cryptosystem without a Trusted Party," in *EUROCRYPT '91*. Springer, 1991, pp. 522–526.

[19] M. Jakobsson and A. Juels, "Mix and Match: Secure Function Evaluation via Ciphertexts," in *ASIACRYPT 2000*. Springer, 2000, pp. 162–177.

[20] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[21] F. Koeune, "Pseudo-Random Number Generator," in *Encyclopedia of Cryptography and Security*, 2005, pp. 485–487.

[22] A. C. Yao, "Protocols for Secure Computations," in *23th Annual Symposium on Foundations of Computer Science (FOCS 82)*. IEEE CS, 1982, pp. 160–164.

[23] S. Ries, "CertainTrust: A Trust Model for Users and Agents," in *ACM Symposium on Applied Computing (SAC 2007)*. ACM, 2007, pp. 1599 – 1604.

[24] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in *IEEE Symposium on Security and Privacy (SP '07)*. IEEE CS, 2007, pp. 321–334.

[25] L. Scott and D. E. Denning, "A Location Based Encryption Technique and Some of Its Applications," in *ION National Technical Meeting 2003*, 2003, pp. 730–740.

[26] A. D. Brucker, H. Petritsch, and S. G. Weber, "Attribute-Based Encryption with Break-Glass," in *Workshop in Information Security Theory and Practice (WISTP'10)*. Springer, 2010, pp. 237–244.

[27] Y. Tsiounis and M. Yung, "On the Security of ElGamal Based Encryption," in *Workshop on Practice and Theory in Public Key Cryptography (PKC '98)*. Springer, 1998, pp. 117–134.

[28] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[29] A. Pfitzmann and M. Hansen, "A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, Dec. 2009, v0.32.

[30] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," in *EUROCRYPT '01*. Springer, 2001, pp. 93–118.

[31] L. A. Martucci, M. Kohlweiss, C. Andersson, and A. Panchenko, "Self-Certified Sybil-Free Pseudonyms," in *Conference on Wireless Network Security (WISEC 2008)*. ACM, 2008, pp. 154–159.

[32] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," in *ACM Conference on Computer and Communications Security (CCS '06)*. ACM, 2006, pp. 99–112.

[33] D. Huang and M. Verma, "ASPE: Attribute-Based Secure Policy Enforcement in Vehicular Ad Hoc Networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1526–1535, 2009.

[34] S. Yu, K. Ren, and W. Lou, "FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks," in *IEEE INFOCOM 2009*. IEEE CS, 2009, pp. 963–971.

[35] C. Andersson, J. Camenisch, S. Crane, S. Fischer-Hübner, R. Leenes, S. Pearsorr, J. Pettersson, and D. Sommer, "Trust in PRIME," in *Intl. Symposium on Signal Processing and Information Technology (ISSPIT 05)*, 2005, pp. 552 – 559.

[36] C. Sorge, J. Girao, and A. Sarma, "Privacy-Enabled Identity Management in the Future Internet," in *FIA Prague 09 (Future of the Internet Conference 2009)*, 2009.