Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy

Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, Günter Müller

Tagging Disclosures of Personal Data to Third Parties to Preserve Privacy

Sven Wohlgemuth[1], Isao Echizen[1], Noboru Sonehara[1], and Günter Müller[2]

[1] National Institute for Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, JAPAN
[2] Institute for Computer Science and Social Studies
Friedrichstr. 50, 79098 Freiburg i.Br., GERMANY
{wohlgemuth,iechizen,sonehara}@nii.ac.jp
mueller@iig.uni-freiburg.de

Abstract. Privacy in cloud computing is at the moment simply a promise to be kept by the software service providers. Users are neither able to control the disclosure of personal data to third parties nor to check if the software service providers have followed the agreed-upon privacy policy. Therefore, disclosure of the users' data to the software service providers of the cloud raises privacy risks. In this article, we show a privacy risk by the example of using electronic health records abroad. As a countermeasure by an ex post enforcement of privacy policies, we propose to observe disclosures of personal data to third parties by using data provenance history and digital watermarking.

1 Introduction

Cloud computing is the modern version of the time-sharing computing model of 1960s, with the main differences being individuals and enterprises make use of services out of the cloud via a web browser and share computing power as well as data storage [14]. Disclosure of users' data to a cloud and at the same time the data federation at software service providers of the cloud facilitate the secondary use of personal data and digital content stored in this, on a massively shared scale, infrastructure, e.g. for data analysis by a third party. The advent of secondary use and disclosure of personal data to third parties have highlighted various problems with cloud computing [20]:

- Legal regulations, such as data protection acts [7, 8, 11], may prohibit the use of clouds for some applications. For instance, the European Data Protection Directive 95/46/EC [7] limits cross-border disclosure of personal data to third countries. An approach is to apply the strictest rules which can restrict the opportunities of cloud computing and increase its costs.
- Even though individuals and companies can protect their information systems by using firewalls and intrusion detection systems, they cannot protect their business processes and data from the software service providers of a cloud. A cloud is a black box: Security processes and data storage are hidden

by the abstraction of the cloud. Users have to trust that the software service providers will follow legal regulations and the agreed-upon policy when using personal data and digital content.

We propose a usage control system for ex post enforcement of privacy policy rules regarding the disclosure of personal data to third parties. Since a cloud has the characteristics of a black box, we assume that personal data has been found at a non-authorized service provider, e.g. during an audit, and the auditor reconstructs the chain of disclosures of personal data in order to identify the party who has violated the obligation. We make use of data provenance [2] and digital watermarking [5] in order to link data provenance history to personal data. Higher cryptographic protocols realizing a traceable linkage of personal data with the data provenance history are our contribution.

Section 2 presents some privacy risks in the case of disclosure of personal data to third parties. Section 3 introduces the concept of using data provenance for usage control. Section 4 presents our privacy preservation system called DETECTIVE and its higher cryptographic protocols. Section 5 reports on the evaluation of our protocols regarding completeness and soundness. Section 6 reports on related work. Section 7 gives an outlook on future work.

2 Privacy Risks by the Example of E-Health

In practice, service providers publish their privacy policy as part of their general terms and conditions. Users have to accept them and thereby give service providers full authority to process their personal data. For instance, a provider of an electronic health record (EHR) data center collects health data from their users (patients) for the purpose of sharing them among others with clinics, health insurance agencies, and pharmaceutical companies [10, 15]. These systems comply with the US American Health Insurance Portability and Accountability Act (HIPAA) [11] by letting users decide on the usage and disclosure of their medical data d, e.g. x-ray images. However, they don't offer mechanisms to enforce the privacy policy rules.

We assume that a patient needs medical treatment abroad. A clinic in the homeland has shot an x-ray image of the patient and has disclosed it to a data center. Patients have shown their digital identity to the first service provider, i.e. the clinic in the homeland, and have agreed on obligations for disclosing their medical data d via a data center to a hospital and to a clinic abroad. Additional disclosures of d are not permitted. Figure 1 shows an exemplary disclosure of the patient's health data d and its modification d' according to the model of [18]. The authorized disclosures are between the clinic in the homeland, a hospital and the clinic abroad via the data center provider. Figure 1 also shows two non-authorized disclosures. The first violation stems from the data center provider; the second violation stems from the clinic abroad. Personal data d has been disclosed to a non-authorized pharmaceutical company. The aim is to identify the data providers who have violated the policy.

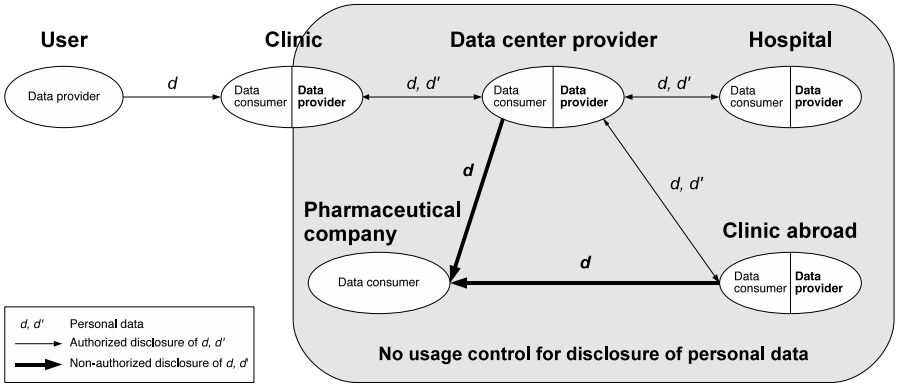

Fig. 1. Some privacy risks in disclosing personal data d to third parties.

3 Usage Control by Data Provenance

After a disclosure of personal data from the corresponding user, access rules to this data are not enforceable anymore by the user's access control system. Usage control extends access control for this purpose by considering access control rules for disclosed data, so called obligations, and the enforcement of obligations [18]. Obligations can be enforced before access to data, e.g. by process re-writing so that violations are impossible, at the moment the data is accessed, e.g. by a monitor with a history of events and knowledge of the future probable process executions, and after an access by an audit [16]. We focus on ex post enforcement, since process re-writing and monitoring contradicts our assumption of a cloud computing information system being a *black box*. Since we want to re-construct the disclosure chain of given data, we make use of data provenance. The aim of data provenance is to identify "where a piece of data came from and the process by which it arrived in a database" [2]. We propose to tag every disclosure of data to a third party with its data provenance information. A sequence of tags for given personal data represents its data provenance history, which is an audit trail. Tagging gives data providers and consumers a proof to show that disclosure and receipt of personal data are done according to the obligations. The data provenance information for d consists of the data provider's, data consumer's identity, and the user's identity as well as a pointer to the obligations. The obligations are indirectly part of a tag by a link to them, since they should be modifiable if the purpose of the data's usage changes or the participating service providers change. The tag should stick to d, similar to [12], so that $d^* = (d, tag)$ can be disclosed while assuring the integrity of the relationship within d^*. If d^* is disclosed further in compliance with the obligations, the tag has to be updated by replacing the identity of the data provider with the identity of the previous data consumer and by adding the new data consumer's identity. The sequence of tags for the same personal data thus constitutes a disclosure chain.

4 DETECTIVE: Data Provenance by Digital Watermarking

Regarding disclosure of personal data to third parties, the one software service provider acting as the data provider embeds data provenance information into the user's personal data to be disclosed by the *DETECTIVE Signaling Module*. Afterwards the tagged data is disclosed to the service provider acting as the data consumer. If subsequent disclosures are allowed by the privacy policy, every software service provider in the disclosure chain should update the data provenance history with the successive data consumer. Regarding a check of the data provenance history, the user or an auditor has found the data. Afterwards, it starts the compliance check of the data's disclosures with the agreed-upon obligations based on the embedded data provenance history. After extracting all digital watermarks of the personal data under investigation, the *DETECTIVE Auditor Module* requests and checks the service providers' input to the data provenance history. The incentive of a service provider, who is acting as a data provider, to tag personal data with the data provenance history is to show his trustworthiness. In section 5 we show that the latest data provider will be identified by a verification of the embedded data provenance history.

4.1 DETECTIVE: The Protocols

DETECTIVE makes use of cryptographic commitments, digital signature, a symmetric digital watermarking algorithm, but without the need of a trustworthy data provider or a trusted third party (TTP) regarding the embedding and checking of data provenance information, and of a protocol for delegation of access rights [1]. The only TTP are the CA for certifying the identities and access rights of all participants and a data protection officer. Cryptographic commitments link the identities of the participating service providers in any disclosure of personal data. Digital signatures are used to establish accountability of the cryptographic commitments to software service providers without opening the commitments. Digital watermarking is used to tag the corresponding personal data with this linkage. Since users do not take part in the disclosures of personal data to third parties, they give their agreement in advance. Hereby, we make us of a delegation of rights protocol. Our scheme consists of the three protocols *Init*, *Tag*, and *Verify*.

Assumptions We assume that proving a digital identity is based on a public-key infrastructure (PKI). We abstract a PKI by making use of one certification authority (CA). This CA certifies the identities and access rights of all participants by issuing credentials. The identities of the user and the participating service providers are represented by their cryptographic secret keys k_{User}, k_{DP}, or k_{DC}, respectively. Concerning a disclosure of personal data, the participants have run a delegation of rights protocol. Accordingly, a data consumer has shown the delegated access rights, which he has got from the user, to the data provider

by means of the $credential_{DC}$. If a data consumer gets access to the requested personal data (the x-ray image of the user in the example), the data provider will use this credential as the watermarking key. The participants have shown their identity, i.e. the ownership of the credential regarding to their identity. Users and service providers have also agreed on a privacy policy including obligations for the disclosure of personal data. Furthermore, the integrity of service providers' systems is ensured by the use of Trusted Computing. The applied symmetric digital watermarking algorithm is robust against modifications of the (cover) data d.

The *Init* Protocol generates a public key pk_{COM}, which is necessary for generating cryptographic commitments and running zero-knowledge proofs. We have chosen protocols based on the discrete logarithm, since we want to commit on strings, i.e. on the participants' cryptographic secret keys, and not a single bit. Both protocols need a public key. This key pk_{COM} consists of two prime numbers p and q and two generators g and h for the group $G_{q,p} : pk_{COM} := (p, q, g, h)$. The corresponding cryptographic key of a data provider is called pk_{DP_COM}.

The *Tag* Protocol runs between a data provider and a data consumer. The aim is to link their identities as well as the obligations for this disclosure to the corresponding personal data d. This protocol consists of the following three phases:

- Phase A: Blinded commitment to the data consumer's identity k_{DC}
- Phase B: Blinded commitment to the data provider's identity k_{DP}
- Phase C: Tagging personal data d with the data provenance information

Figure 2 shows the messages of phase A. The first two steps are necessary for the data consumer to commit to k_{DC}. The data consumer commits to his identity k_{DC} by $com_{DC}(k_{DC})$, whereas m is chosen at random out of the group $\mathbf{Z_q}$. We use $com_{DC}(k_{DC})$ for linking it with the data provider's identity. The constraint is that only the data consumer will get the resulting commitment to this disclosure of d. Hence, we later compute the product of two commitments and extract from this product a secret value of the data consumer. Therefore, we blind $com_{DC}(k_{DC})$ with the blinding factor $com_{DC}(b)$. The result is $com_{DC\_BLINDED}(k_{DC})$. This blinding is similar to blind digital signature systems, e.g. as they are used for electronic coins [4]. The data consumer chooses the secret values b and l at random out of $\mathbf{Z_q}$. Next, the data consumer confirms the relationship of his inputs to him by digitally signing his identity $com_{DC\_BLINDED}(k_{DC})$ and the transcript of the protocol run for showing $credential_{DC}$. Afterwards, the data consumer sends the blinded commitment to k_{DC} and this digital signature to the data provider.

Phases B and C aim at linking the identities of the data consumer and provider to the user's personal data d (cf. Figure 3). The data provider verifies $com_{DC\_BLINDED}(k_{DC})$ and the confirmation of the data consumer. Afterwards it computes $com_{DP\_BLINDED}(k_{DP})$ which represents the source of the data

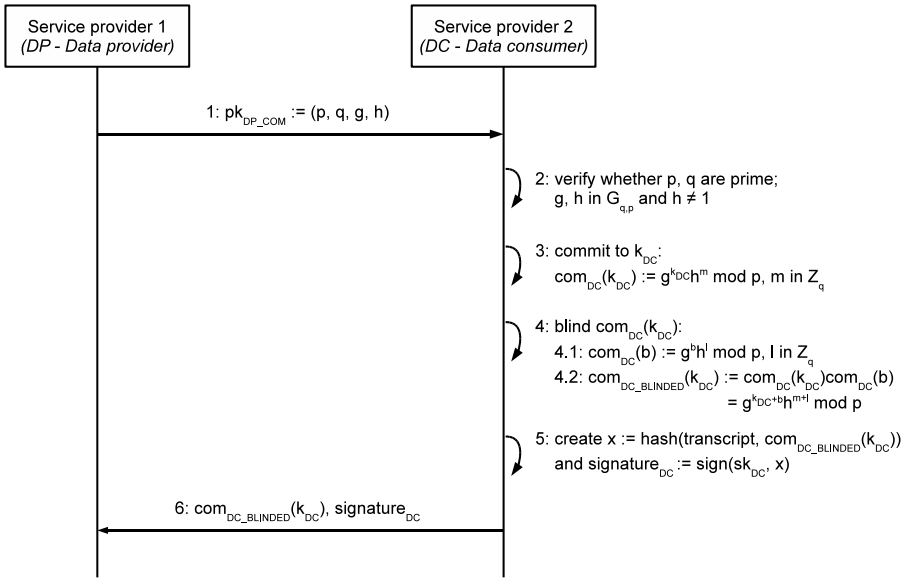

Fig. 2. Phase A of the DETECTIVE *Tag* protocol.

disclosure. The function $fing_{sym}$ represents the call of the symmetric digital watermarking algorithm's embedding function. The selection of the watermarking algorithm depends on the medium type of the personal data. The result of $fing_{sym}$ is wm', the blinded data provenance information concerning this part of the disclosure chain of the user's personal data d. Before sending wm' to the data consumer though, the data provider confirms that he has used his master identity k_{DP} by digitally signing it together with the transcript of the delegation of rights protocol run. The data consumer reveals the resulting digital watermark wm by extracting wm', checking the digital signature $signature_{DC}$ of the data provider, removing his blinding factor $com_{DC}(b)$ from the data provenance information and embedding the resulting data provenance information dpi as the digital watermark wm, which is the unblinded wm', into d.[3]

The *Verify* Protocol aims at identifying the service provider who has done an unauthorized disclosure of the found user's data. It works by checking the cryptographic commitments of the found data and the digital signature of the participating data provider and consumer. The participants of the protocol *Verify* are an auditor (data protection officer), the CA, a data consumer, and a data provider of the corresponding disclosure chain. The auditor runs this protocol, if he has found personal data at a service provider who is not authorized to get this data. The protocol *Verify* consists of the following three phases:

[3] The data consumer knows the watermarking key $credential_{DC}$ from the delegation of rights protocol.

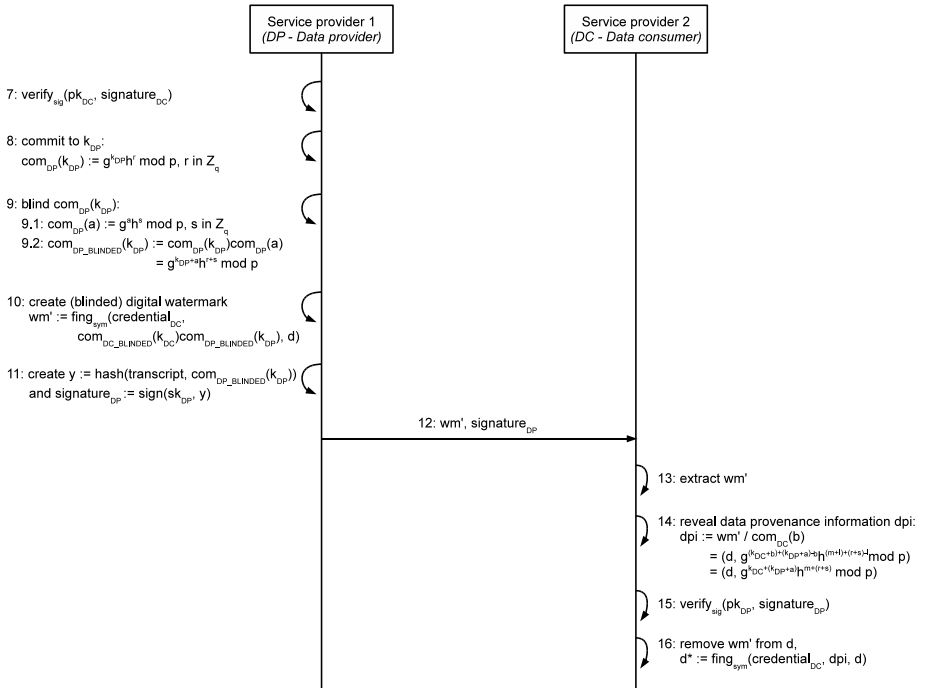

Fig. 3. Phases B and C of the DETECTIVE *Tag* protocol.

- Phase D: Retrieving the used watermarking keys for the disclosure of the found user's data d
- Phase E: For each digital watermark of d: Checking the data provider's cryptographic commitment for the resulting tag
- Phase F: For each digital watermark of d: Checking the data consumers commitment

The aim of phase D is to get the credentials of the authorized data consumers to extract all watermarks of the found data d. The cryptographic commitments are checked in phases E and F, as shown in Figure 4. In phase E, the auditor checks the commitment and digital signature of the data provider by re-calculating it. If the result equals $com_{DP\_BLINDED}(k_{DP})$, then it belongs to this service provider. Since the secret key k_{DP} is blinded by the addition with the blinding factor a, the auditor will not know k_{DP}: An addition modulo p is a one-time pad encryption which is information-theoretical secure if the encryption key in this case the attribute a is used only once.

Phase F aims at determining recursive in the disclosure chain of d whether the last service provider acting as a data provider or the last service provider acting as a data consumer has further disclosed d. The auditor retrieves the data consumer's commitment $com_{DC\_BLINDED}(k_{DC})$ by dividing the extracted cryptographic commitment with the blinded commitment of the data provider.

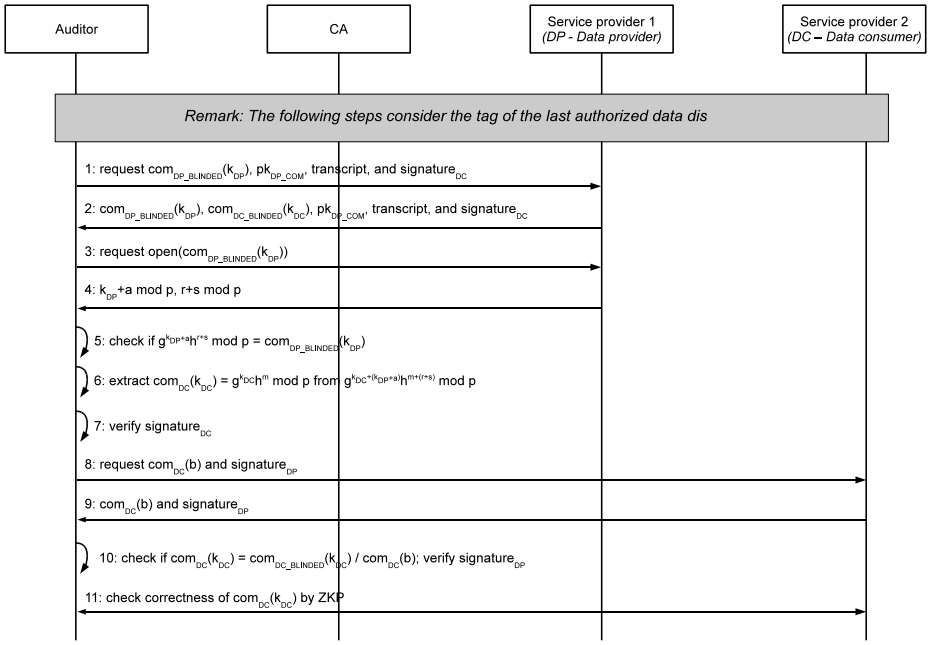

Fig. 4. Phases E and F of the DETECTIVE *Verify* protocol.

Then the auditor checks the digital signature of the data consumer. If this digital signature is correct, then $com_{DC\_BLINDED}(k_{DC})$ belongs to this data consumer. To verify that this data consumer has used $com_{DC\_BLINDED}(k_{DC})$ in the *Tag* protocol, the auditor checks if it refers to $com_{DC}(k_{DC})$ by requesting the blinding factor $com_{DC}(b)$ from the data consumer and re-calculating $com_{DC}(k_{DC})$. Since the master identity of the data consumer should be kept confidential, the casual way of showing the correctness of a commitment simply by opening this commitment is not possible. Hence, the service provider shows its correctness by performing a zero-knowledge proof.

5 Properties of the DETECTIVE Protocols

Concerning the correctness of the DETECTIVE protocols, we have to show that they fulfill the properties of completeness and soundness as follows:

- Completeness: A honest service provider acting as the data provider can convince a honest auditor that the service provider acting as the data consumer in the case of a non-authorized disclosure of d is dishonest.
- Soundness: Dishonest service providers cannot convince a honest auditor that they have not disclosed personal data d to non-authorized service providers, if the auditor has found d at a non-authorized service provider.

5.1 Completeness

A dishonest service provider has disclosed the user's personal data d further without adding the new data provenance information for the upcoming disclosure, i.e. this service provider has not run the *Tag* protocol. In figure 1, this could be the data center provider or the clinic abroad. Since the previous service provider, the homeland clinic, was authorized by the user to collect d, this service provider has an incentive to follow the *Tag* protocol. Hence, the homeland clinic has given correct values to the protocol and proven the correctness of the next data consumer's digital signature regarding the data consumer's $com_{DC\_BLINDED}(k_{DC})$. The auditor knows the identity of this data consumer due to the corresponding delegated access right of the user. If the data consumer's digital signature is valid, the accountability of $com_{DC\_BLINDED}(k_{DC})$ is assured. Next the auditor checks the relationship of $com_{DC\_BLINDED}(k_{DC})$ to k_{DC}. Because of the soundness property of zero-knowledge proofs, the proving party (data consumer) cannot cheat in a zero-knowledge proof [9]. If $signature_{DC}$ and $com_{DC}(k_{DC})$ are correct and $com_{DC\_BLINDED}(k_{DC})$ is part of the last digital watermark of d, then it is an evidence that the data provider has disclosed d to this non-authorized data consumer. Otherwise the auditor runs the phases E and F of the *Verify* protocol for the previous digital watermark in this disclosure chain. If the next digital watermark is the last one concerning the disclosure chain of d and the attributes of the data provider and of the data consumer are correct, then the first data consumer has disclosed d to the non-authorized party.

5.2 Soundness

Both service providers involved in the disclosure of d have violated the obligations. They aim to conceal their identities as the data provider by either modifying the tag of the previous disclosure or by cheating in the *Tag* protocol. We consider the following attacks:

(a) Removing the digital watermark of the previous disclosure of d
(b) Further disclosure of d without adding the new digital watermark regarding this disclosure
(c) Tagging of d with a cryptographic commitment to another value than k_{DC} or k_{DP}

Service providers who participate in a disclosure of d know the watermarking key. Regarding the attack (a), if the data provider wants to conceal his violation, he could remove the tag of the previous disclosure. This is possible as long as the previous data provider is dishonest, too. Even though if this happens recursive in the disclosure chain until the first data consumer, an auditor detects the dishonest behavior of the first data consumer. The reason is that the auditor has got the cryptographic commitment of this service provider's identity k_{DC} and his digital signature on the commitment and the protocol run of showing his rights to access d by his credential. Also, this service provider has proven to

the first data provider that its commitment refers to k_{DC}. This forces at least the first data provider to follow the *Verify* protocol.

Regarding the attack (b), at least the second data consumer in a disclosure chain has disclosed d to a non-authorized participant. If the last data consumer in the disclosure chain has disclosed d, it will be identified as the dishonest service provider because of the completeness property of the DETECTIVE protocols. If it was the last data provider, then this participant will be identified as the violator due to the digital watermark for the disclosure of d from the previous data provider and the completeness property of the DETECTIVE protocols.

Concerning the attack (c), since a commitment relates to another value than k_{DC} or k_{DP}, the cheating party either cannot convince an auditor in the opening protocol of the cryptographic commitment or in the zero-knowledge proof. If the data consumer has used an invalid commitment and the data provider has accepted it, then the auditor would identify the data provider as the violator since the data consumer cannot prove the knowledge of k_{DC} to the commitment $com_{DC}(k_{DC})$. If the digital signature of the data provider does not refer to the data providers commitment, then the data provider has not followed the *Tag* protocol. Even if the data provider has used a commitment different to k_{DP} but it knows the committed value, then it can still show his role as the data provider. But if it has not used this commitment in the *Tag* protocol, then it is not part of the digital watermark and the auditor cannot extract the correct $com_{DC}(k_{DC})$.

6 Related Work

Enforcement mechanisms for policies regarding information flows concentrate on formal methods [13] or on encryption [3]. Formal methods consider information flows via covert channels or an indirect path from a data provider to a data consumer. In addition, a corresponding verification of a system implies that this system doesn't change afterwards. Otherwise, it has to be verified again. Combining personal data with obligations is the characteristic of a sticky policy [12]. An implementation of sticky policies for disclosure of personal data to third parties is the Adaptive PMS of Hewlett-Packard [3]. Sticky policies are linked to certain personal data at the time of their collection by an encryption scheme. A data consumer will get the decryption key from a TTP, if it is authorized by the sticky policy. However, data consumers can further disclose the decrypted personal data without any control by the user or the TTP.

The main characteristic of the symmetric watermarking scheme is the use of a symmetric watermarking key in order to produce noise in which a digital watermark is to be embedded [5]. If one knows this key and the watermarking algorithm, he can embed, detect, and modify watermarks. If a symmetric digital watermarking scheme is applied to our scenario, both the data provider and consumer get the same digital watermark. This means that if one of them discloses this personal data to a third party, an auditor cannot decide whether the data provider or the data consumer has violated this obligation. Digital watermarking for tracing disclosure of health data has been used for medical images according

to the DICOM standard [6]. The watermarking scheme uses a TTP for the generation and distribution of the personalized watermarking keys for each authorized consumer as well as for checking a digital watermark. By subtracting the personalized watermarking key of the recipient from the data center provider's digital watermark, every authorized data consumer gets the same medical image with a personalized digital watermark. However it is assumed that every data consumer will subtract his watermarking key from the received image. If two or more data consumers won't follow the subtraction rule, they would be indistinguishable since they have the same digital watermark.

Asymmetric fingerprinting [17] solves this problem of indistinguishability in the context of DRM. In principle, it combines a symmetric watermarking scheme with cryptographic commitments and digital signature. Data providers embed the digital watermarks consisting of a random identity chosen by data consumers. The protocol of asymmetric fingerprinting assures, because of computing with cryptographic commitments, that only data consumers get the watermark. The obligations are signed by data consumers and sent to the data provider. However, asymmetric fingerprinting assumes conflicting interests of providers and consumers. This contradicts to our trust model. Service providers may hide the correct watermarking key, since they have an interest to collude.

7 Conclusion

Our proposal of usage control through data provenance enables users to check ex post whether software service providers are actually obeying and enforcing obligations. Therefore, we have presented a modified asymmetric fingerprinting scheme called DETECTIVE. In the future, we will evaluate the feasibility of our scheme by a proof-of-concept implementation for the case study "Telemedicine" in which personal data (x-ray images) are sent from a clinic in the homeland to a clinic abroad via a data center as a cloud service. The feasibility evaluation will show if the same number of digital watermarks as the number of disclosures of a disclosure chain can be embedded into an x-ray image while remaining the digital watermarks detectable and extractable for an auditor as well as remaining the x-ray image usable for the medical institutions. Also we will investigate whether a modification of personal data, e.g. updating an electronic health record, will modify the embedded data provenance history.

Acknowledgment

This work was funded by the German Academic Exchange Service (DAAD) and is a result of the Memorandum of Understanding between the National Institute of Informatics (Japan) and the Albert-Ludwig University of Freiburg (Germany). We would like to thank Jérémie Tharaud and the reviewers of IFIP SEC 2010 for their valuable comments.

References

1. Aura, T., Distributed Access-Rights Managements with Delegations Certificates. In: Secure Internet Programming. LNCS 1603, Springer, pp.211–235 (1999)
2. Buneman, P., Khanna, S., and Tan, W-C., Why and Where: A Characterization of Data Provenance, ICDT 2001, LNCS Vol. 1973, Springer, pp. 316–330 (2001)
3. Casassa Mont, M. and Pearson, S., An Adaptive Privacy Management System for Data Repositories, TrustBus 2005, LNCS 3592, Springer, pp. 236–245 (2005)
4. Chaum, D., Blind Signatures for Untraceable Payments, In Advances in Cryptology – Proceedings of Crypto '82, Springer, pp. 199–203 (1982)
5. Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J., and Kalker, T., Digital Watermarking and Steganography, Morgan Kaufmann (2008)
6. Li, M., Poovendran, R., and Narayanan, S., Protecting patient privacy against unauthorized release of medical images in a group communication environment, Comp. Medical Imaging and Graphics, Vol. 29, Elsevier, pp. 367–383 (2005)
7. European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, L 281, 395L0046, pp. 31–50 (1995)
8. Deutscher Bundestag. Gesetz zur Modernisierung der gesetzlichen Krankenversicherung. Bundesgesetzblatt Jahrgang 2003 Teil I Nr. 55 (2003)
9. Goldwasser, S., Micali, S., and Rackoff, C., The knowledge complexity of interactive proof systems, SIAM J. Computation 18(1), pp.186–208 (1989)
10. Google, Health Privacy Policy, http://www.google.com/health (2010)
11. U.S. Department of Health & Human Services, Health Insurance Portability and Accountability Act of 1996 Privacy Rule, http://www.cms.hhs.gov/HIPAAGenInfo (1996)
12. Karjoth, G., Schunter, M., and Waidner, M., Privacy-enabled Services for Enterprises, 13th Int. Workshop on Database and Expert Systems Applications, IEEE Computer Society, pp. 483–487 (2002)
13. Mantel, H., Information Flow Control and Applications Bridging a Gap, FME 2001, LNCS 2021, Springer, pp. 153–172 (2001)
14. Mather, T., Kumaraswamy, S., and Latif, S., Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, OReilly Media (2009)
15. Microsoft, HealthVault Privacy Policy, http://www.healthvault.com (2010)
16. Müller, G., Accorsi, R., Höhn, S., and Sackmann, S., Sichere Nutzungskontrolle für mehr Transparenz in Finanzmärkten, Informatik-Spektrum 33(1), Springer (2010)
17. Pfitzmann, B. and Schunter, M., Asymmetric Fingerprinting, EUROCRYPT 1996, LNCS 1070, Springer, pp. 84–95 (1996)
18. Pretschner, A. Hilty, M., and Basin, D., Distributed usage control, CACM 49(9), ACM Press, pp. 39–44 (2006)
19. Sackmann, S., Strüker, J., and Accorsi, R., Personalization in Privacy-Aware Highly Dynamic Systems, CACM 49(9), ACM Press, pp. 32–38 (2006)
20. Sonehara, N., Echizen, I., Wohlgemuth, S., Müller, G., and Tjoa, A. (eds), Int. Workshop ISSI 2009, http://www.nii.ac.jp/issi, National Center for Sciences (2009)