Journal of Information Hiding and Multimedia Signal Processing ©2011 ISSN 2073-4212
Ubiquitous International Volume **2**, Number **3**, July **2011**

On Privacy-compliant Disclosure of Personal Data to Third Parties using Digital Watermarking

Sven Wohlgemuth, Isao Echizen and Noboru Sonehara

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
wohlgemuth@nii.ac.jp; iechizen@nii.ac.jp; sonehara@nii.ac.jp

Günter Müller

Institute of Computer Science and Social Studies (Telematics)
Albert-Ludwig University of Freiburg
Friedrichstr. 50, 79098 Freiburg i.Br., Germany
mueller@iig.uni-freiburg.de

Received June 2010; revised February 2011

Abstract. *Privacy in business processes for providing personalized services is currently a matter of trust. Business processes require the disclosure of personal data to third parties and users are not able to control their usage and so their further disclosure. Existing privacy-enhancing technologies consider access control but not usage control of personal data. The current work on usage control mainly considers formalization of usage rules, i.e. obligations, and their enforcement by using the mechanisms of digital rights management, secure logging of access requests for ex post enforcement, and non-linkable delegation of access rights to personal data. However, either these enforcement mechanisms do not consider a disclosure of personal data to third parties or they assume trustworthy data consumers or data providers. We investigate on digital watermarking as a way of enforcing obligations for further disclosure of personal data without mandatory trust in service providers.*
Keywords: Privacy, Business Processes, Data Provenance, Digital Watermarking

1. **Introduction.** Business processes for providing personalized services require the collection of personal data and their disclosure to third parties. Depending on the service and thereby on the purpose of a personal data's usage, service providers act as a data consumer or as a data provider. As a data consumer they collect, process, and store personal data. As a data provider they disclose personal data to other service providers. Examples illustrating this role change of service providers depending on the purpose are medical services with electronic health records. The challenge is whether the requirements of data protection legislations, e.g. the European Data Protection Directive [1] and US American Health Insurance Portability and Accountability Act (HIPAA) [2], can be fulfilled so that users can enforce the agreed-upon rules concerning the usage of their data. Concerning the disclosure of personal data to third parties, the user has to give his agreement in advance. In practice, users agree to the privacy policy of service providers and the service providers promise to follow it.

Technically, the rules of a privacy policy correspond to provisions and obligations to get access to some personal data. Whereas provisions formalize conditions for access to data and are enforceable by users, obligations formalize rules for their usage, e.g. disclosure,

and are not enforceable by the user at the time of the access. But in principle obligations are observable afterwards [3]. However, existing privacy-enhancing technologies, e.g. anonymity services and identity management systems, focus on the collection of personal data and hence on the access to them [4]. For instance, identity management protects users against non-authorized profiling by the provision of pseudonymity. However, if identity management systems are used for a disclosure of personal data to third parties, users have to share their master identity with data consumers. Hence they will lose the control over their personal data [5]. Approaches of privacy-preserving technologies for a disclosure of personal data to third parties focus on obscurity by encryption and private information retrieval [6]. Encrypted data hinders the identification of the corresponding user and it can be used for statistic analysis. Private information retrieval assures that users remain non-linkable if disclosed personal data is requested. But these approaches have the drawbacks that (a) this data protection is not suitable if services require identifiable personal data and (b) data is not protected anymore after its decryption. Even though the DREISAM protocols for a non-linkable delegation of rights to access personal data allow a selective disclosure of personal data to third parties without demanding trust in data consumers, they assume that data providers will enforce delegated rights and thereby that users trust them [5].

Current work on usage control is mainly engaged in enforcement mechanisms of Digital Rights Management (DRM) and secure logging by either focusing on the processing of data or on detecting unauthorized copies [7]. DRM monitoring mechanisms require control of data consumers?information systems for restricting the usage of data by an access control system. Since they follow the white box approach, they are not suitable for a privacy-preserving disclosure of personal data to third parties: It cannot be assumed that users get control on an information systems of a service provider. DRM mechanisms for detecting unauthorized copies follow the black box approach and require trustworthy signals concerning unauthorized copying, i.e. violations of obligations. But they do not consider a selective disclosure of data to third parties.

In this article, we will discuss the suitability of digital watermarking as an instrument for observing a chain of disclosures of personal data to third parties. We present our scheme DETECTIVE. The novelty of DETECTIVE is the tagging of disclosures of personal data to third parties by using digital watermarking but without a Trusted Third Party (TTP) regarding the embedding of digital watermarks.

2. **Privacy and Disclosure of Personal Data to Third Parties.** 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 a data center for electronic health records such as Microsoft HealthVault[1] and Google Health[2] collects health data of their users for sharing them among others with clinics, health insurance agencies, and pharmaceutical companies. These systems comply with HIPAA by letting the users decide on the usage and disclosure of their medical data, e.g. x-ray images. But they do not offer mechanisms to guarantee this kind of compliance of their system especially regarding the enforcement of users?decisions. We assume that a clinic has shot an x-ray image of a user and disclosed it to a data center for sharing it with an external medical specialist. We assume further that users have shown their identity to the first data consumer, i.e. the local clinic, and have agreed on obligations for disclosure of their medical data d via a data center to

[1] cf. http://www.healthvault.com

[2] cf. http://www.google.com/health

a hospital and to a medical specialist. Additional disclosures of d are not permitted, especially not to a pharmaceutical company.

Figure 1 shows an exemplary disclosure of the users data according to the role model of Pretschner et al. [3] and two violations of the agreed-upon obligations. Authorized disclosures of d and its modification d are between the local clinic, hospital and a clinic abroad via a data center provider. The first violation in figure 1 stems from the data center provider. This provider has disclosed d to a pharmaceutical company. The second violation stems from the clinic abroad due of disclosing d to a pharmaceutical company. The challenge is to detect non-authorized disclosures of personal data and to identify those data providers who have violated the agreed-upon privacy policy.

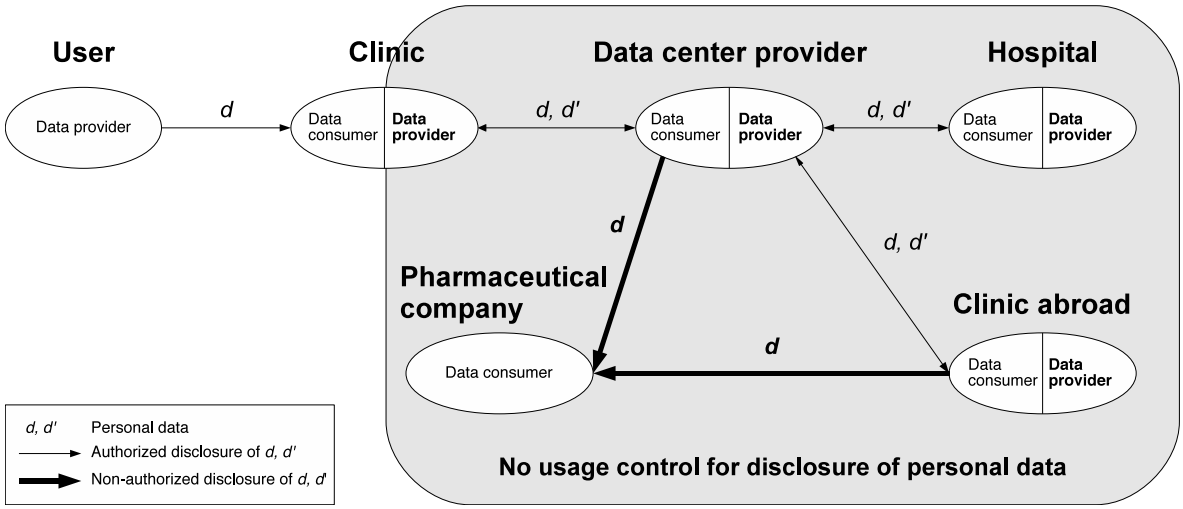

FIGURE 1. Exemplary disclosures of personal data to third parties.

3. **Observation of a Data Disclosure to Third Parties.** Since it is unlikely that service providers will give users control over their information system, we treat their information system as a black box. Our approach assumes that a service provider has already collected some personal data. It focuses on the observation of disclosures of given personal data between at least two service providers. To identify a disclosure of personal data between these participants, a flow of personal data should be *traceable*. Moreover, to prevent indirect data flows, users?transactions should be *non-linkable* as far as obligations do not consider the disclosure of identifying data to third parties. *Traceability* in this context means that a personal data flow should be uniquely mapped to the data providers, data consumers, and the corresponding user. Data providers should not be able to repudiate a disclosure (*non-repudiation*); they should be able to prove that they have not disclosed given personal data to certain third parties. We propose to tag a flow of personal data d between two parties and to get a proof for data providers and data consumers concerning the disclosure and receipt of given personal data. The tag should be *sticky* to d similar to Karjoth et al. [8] so that $d^* = (d, tag)$ can be disclosed while assuring the integrity of d^*. A tag consists of data providers identity (ID_{DP}), data consumers identity (ID_{DC}), the corresponding users identity (ID_{User}), and of a pointer ($link_{Obligations}$) to the agreed-upon obligations. The obligations are indirectly part of a tag, since they should be modifiable without re-tagging the data due to a change of the business process or authorized service providers. If d^* has been disclosed further in compliant to the obligations, the tag has to be updated by adding the identity of the previous

data consumer as the new data provider ID_{DP} and the identity of the new data consumer ID_{DC}. A sequence of tags for the same personal data d describes its chain of disclosures.

Tagging personal data is not enough for checking service providers?compliance with the agreed-upon privacy policy regarding disclosures of personal data to third parties. In particular since users cannot influence the enforcement of tagging personal data without having access to service providers?information system or demanding authentic events, e.g. to their decisions regarding access requests to personal data. The idea of our system is that trustworthy service providers will get a tool for showing their compliance to the agreed-upon privacy policy to their users and to an arbiter. This means that

- Tags must be checkable by the user or an arbiter and
- The checking process must fulfill completeness and soundness.

We define completeness and soundness as follows:

- Completeness: An honest service provider acting as a data provider can convince an honest user 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 an honest user that they have not disclosed personal data d^* to non-authorized service providers if the user or a third party, e.g. a data protection officer, has found d^* at a non-authorized service provider.

4. **Related Work.** Related work on enforcement of policies for data (information) flows concentrate on formal methods [9] or on encryption [10]. However 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 won't be changed afterwards. Otherwise, it has to be verified again. Combining personal data with obligations to their usage is the characteristic of a sticky policy. An implementation of sticky policies for disclosure of personal data to third parties is the adaptive privacy management system (Adaptive PMS) of Hewlett-Packard [10]. Sticky policies are linked to certain personal data at the time of their collection by an encryption scheme. An authorized data consumer will get the decryption key from a TTP. However, data consumers can further disclose the decrypted personal data without any control by the user or the TTP.

Digital watermarking is used to detect unauthorized copies and modification of digital content as well as for confidential data transmission [11]. The main characteristic of the symmetric digital watermarking scheme is the use of a symmetric watermarking key in order to produce noise in which a digital watermark is to be embedded. If one knows this key and the watermarking algorithm, one can embed, detect, and modify watermarks. If a symmetric digital watermarking scheme is applied to our model, e.g. in the example of medical services with electronic health records, both the data provider and the data consumer get the same digital watermark due to the symmetry of digital watermarking. This means that if one of them discloses this personal data to a third party, the user cannot decide whether the data provider or the data consumer has violated this obligation. For this reason, a TTP has to be introduced in order to embed and detect digital watermarks so that only the TTP knows these secrets. However, every participant has to trust the TTP that she will embed and detect digital watermarks according to her policy.

In the context of DRM, asymmetric fingerprinting [12] solves this problem of indistinguishability. In principle, it combines a symmetric watermarking scheme with cryptographic commitments and the digital signature. Data providers embed the digital watermarks consisting of a random ID_{DC} chosen by the data consumer together with a

text, here the obligations. The protocol of asymmetric fingerprinting assures, by using cryptographic commitments, that only data consumers get the digital 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 violate the agreed-upon obligations, since they have an interest to collude. A solution is again the introduction of a TTP who checks whether data providers and data consumers have run the asymmetric fingerprinting protocol as expected by verifying the results of the protocol.

Digital watermarking for tracing disclosure of health data has been used for medical images according to the DICOM (Digital Imaging and Communication in Medicine) standard [13]. That study considers a closed group of data providers and consumers. 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 providers 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 did not follow the subtraction rule, they would be indistinguishable since they have the same watermark.

5. DETECTIVE: Detecting Non-Authorized Disclosures of Personal Data to Third Parties.

We propose a scheme called DETECTIVE without a TTP regarding embedding digital watermarks. Our scheme makes use of cryptographic commitments, zero-knowledge proof, and of a symmetric digital watermarking algorithm but without the need of mandatory trustworthy data providers and a TTP. Cryptographic commitments link the identities of the participating service providers in a disclosure of personal data. Zero-knowledge proofs are used as a showing of a commitment's sub protocol to verify the knowledge of a service provider's identity (secret cryptographic key k). Digital watermarking is used to tag the corresponding personal data with this link. Since users do not take part in a delegation of his personal data, they give their agreement in advance. Hereby, we make us of the delegation protocol DREISAM for a non-linkable delegation of rights to ensure that no additional data of the user will be disclosed at the time of users authentication and consent for data consumers to access users personal data at a data center. Our scheme consists of the three protocols *Init*, *Tag*, and *Verify*.

We assume that proving an identity is based on a public-key infrastructure for anonymous credentials [14]. The identities of the user and the participating service providers are represented by their cryptographic secret key k_{User} or $k_{ServiceProvider}$ respectively. Concerning the disclosure of users personal data, we assume that the participants have run the delegation protocol DREISAM. Thereby a data consumer has shown the delegated access rights, which he has got from the user, to the data provider by means of $anonymousCredential_{DC}$. By this credential, the rule of the privacy policy according to this disclosure is linked ($link_{Obligations}$). If a data consumer gets access to the requested personal data d (in the example the x-ray image of a patient), the data provider will use $anonymousCredential_{DC}$ as the watermarking key in the protocol *Tag*. Furthermore, we assume that the participants have shown their identity, i.e. 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.

5.1. The Protocol *Init*.

The protocol *Init* generates a public key pk_{COM}, which is necessary for cryptographic commitments and 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 key, and not a single bit. Both protocols assume a public key of the recipient of a message. According to the specification of these protocols [15] pk_{COM} consists of two prime numbers p and q and of two generators g and h for the group $G_{q,p} : pk_{COM} := (p, q, g, h)$. According to the role of a participant as a data provider in our protocols, the corresponding key is called $pk_{DP_{COM}}$.

5.2. **The Protocol *Tag*.** The protocol *Tag* runs between a data provider and a data consumer. The aim is to link the data providers and data consumers identity and the obligations for this disclosure to the corresponding personal data d (the patients x-ray image). To distinguish between a service provider as data provider and a service provider as data consumer, the identity of the data provider or data consumer is represented by the cryptographic commitment to his secret key k_{DP} or k_{DC}. respectively. The data provider multiplies these cryptographic commitments and embeds the resulting product in the personal data d. The data provider uses a symmetric digital watermarking scheme in order to embed the multiplied commitments. This is not the resulting digital watermark, since the data provider would also have it. Therefore, the data consumer opens his commitments. The result is the product of data provider's commitment with the opened data consumers commitments. This is the watermark of the personal data. On the other side, the data provider needs a confirmation that he has got the identity of the data consumer, i.e. his commitments, and the rights which the data consumer has got from the user. The data consumer gets a confirmation of the data provider that the data provider has used a commitment to his identity k_{DP} for this digital watermark. This requirement of non-repudiation is fulfilled by the digital signature for the *transcript*, which consists of the messages of a run of the credential's showing protocol, and the cryptographic commitments concerning k_{DC} and k_{DP}. After getting the signature and commitment of the data consumer, the data provider will compute the commitment of the embedded data and send it to the data consumer. This protocol consists of the following three phases:

- Phase A: Blinded commitment to the data consumers identity k_{DC}.
- Phase B: Blinded commitment to the data providers identity k_{DP}.
- Phase C: Tagging personal data d.

Figure 2 shows the protocol flow for the *phase A*. The first two steps necessary for the data consumer to be able to commit to k_{DC}. The data consumer commits to his identity k_{DC} by computing the commitment $com_{DC}(k_{DC}) := g^{k_{DC}} h^m \ mod \ p$, whereas m is chosen at random out of the group $\mathbf{Z_q}$. It would be sufficient if $com_{DC}(k_{DC})$ were exclusively used to commit to the data consumer's identity. However, we shall use it 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 $com_{DC}(b) := g^b h^l \ mod \ p$. The data consumer chooses the secret values b and l at random out of $\mathbf{Z_q}$. The resulting blinded commitment to k_{DC} is: $com_{DC\_BLINDED}(k_{DC}) := g^{k_{DC}+b} h^{m+l} \ mod \ p$. Next, the data consumer confirms the relationship of his inputs by digitally signing the cryptographic commitment to his identity $com_{DC\_BLINDED}(k_{DC})$ and the transcript of the protocol run for showing $anonymousCredential_{DC}$.

The *phases B and C* aim at linking the identities of the data consumer and provider to the user's personal data d (x-ray image). Figure 3 shows their message flows. The data provider verifies $com_{DC\_BLINDED}(k_{DC})$ and the confirmation of the data consumer. The commitment $com_{DP\_BLINDED}(k_{DP})$ represents the source of the data disclosure. The generation of this commitment is the same as it is for the data consumer. The function

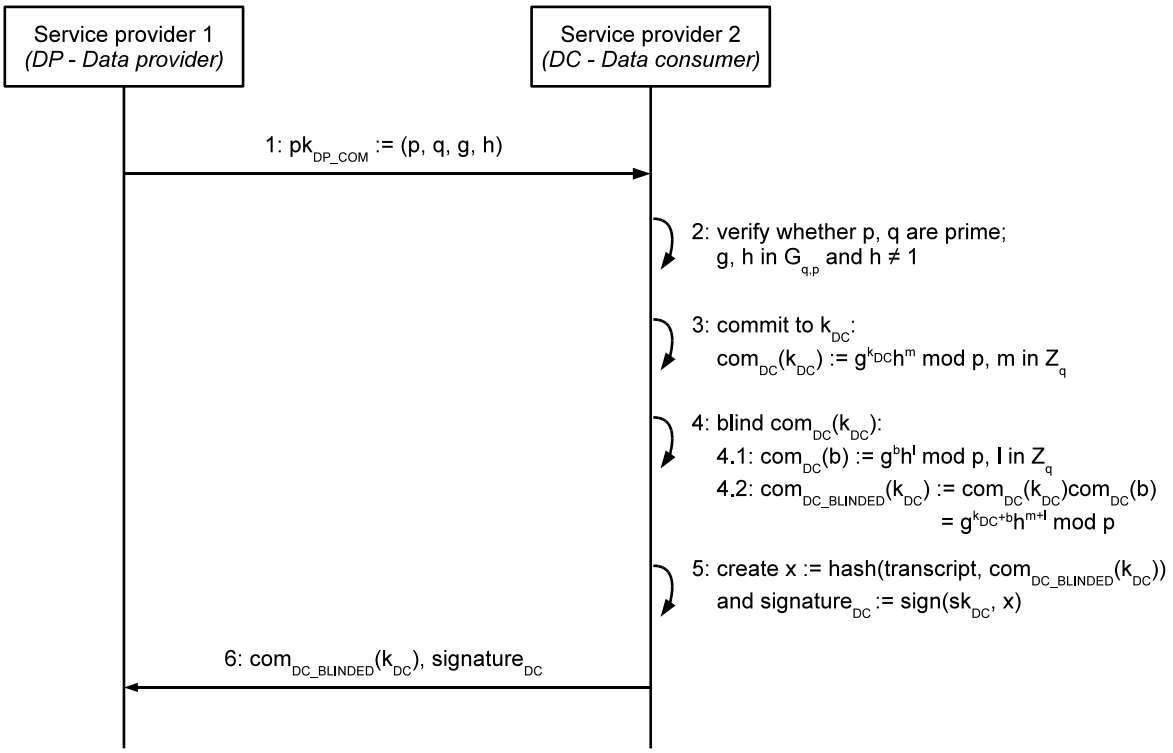

FIGURE 2. Phase A of the DETECTIVE *Tag* protocol.

$fing_{sym}$ represents the call of the symmetric digital watermarking algorithm's embedding function, which depends on the medium type of the personal data, e.g. DICOM. 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, the data provider confirms that he has used k_{DP} by digitally signing it together with the transcript of the DREISAM protocol run. The data consumer reveals the resulting digital watermark wm by removing his blinding factor $com_{DC}(b)$.

5.3. **The Protocol *Verify*.** The aim of the protocol *Verify* is to identify the service provider disclosing the found user's data who made an unauthorized disclosure of the found user's data. It checks the cryptographic commitments of the found data, which had been embedded with the protocol *Tag*, and the digital signature of the service provider acting as the data consumer in this disclosure. The participants of the protocol *Verify* are the user, the CA, a data consumer, and a data provider of the corresponding disclosure chain. The user runs the protocol *Verify*, if he has found personal data at a service provider who is not authorized to get this data. This protocol *Verify* consists of the following three phases:

- 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 anonymous 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 user checks the commitment and digital signature of the data provider by re-calculating it with the generators

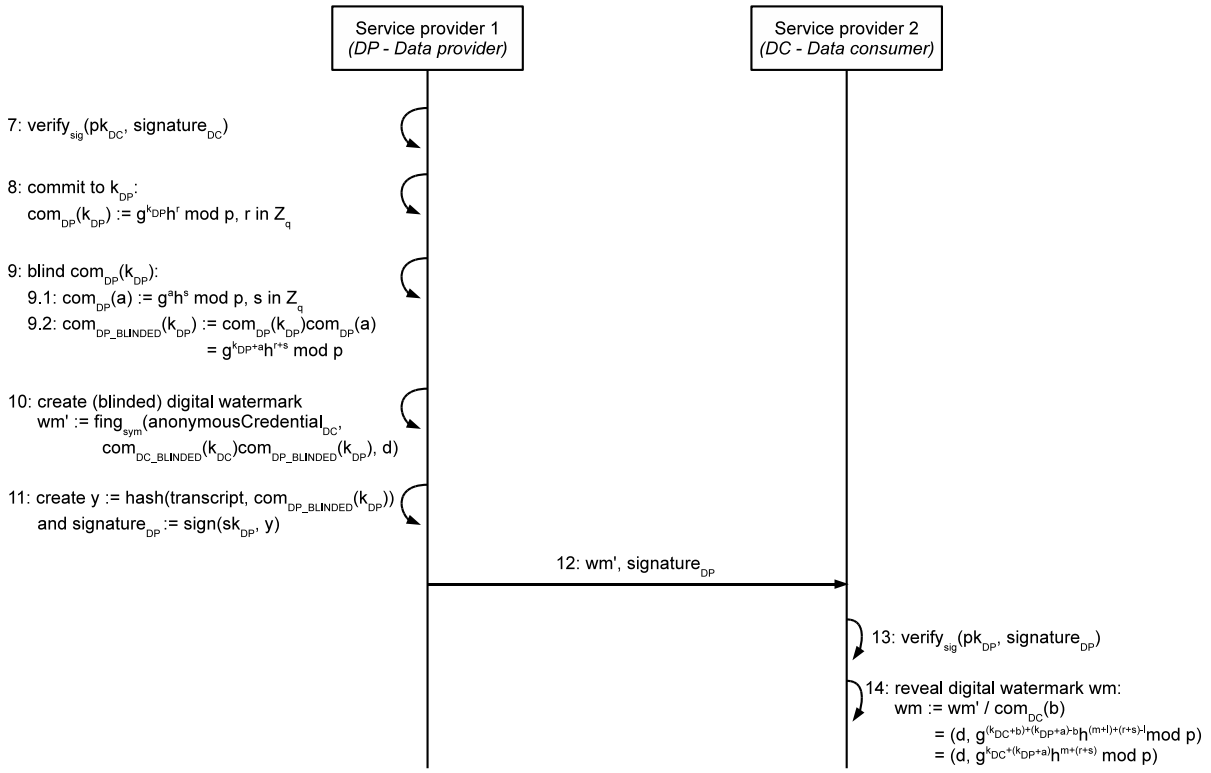

FIGURE 3. Phases B and C of the DETECTIVE *Tag* protocol.

g and h, the prime number p, and the received values $k_{DP} + a \ mod \ p$ and $r + s \ mod \ p$. 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 user 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.

The *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 the personal data d. The user retrieves the data consumer's commitment $com_{DC\_BLINDED}(k_{DC})$ by dividing the extracted cryptographic commitment $g^{k_{DC}+(k_{DP}+a)}h^{m+(r+s)} \ mod \ p$ with the blinded commitment of the data provider $g^{k_{DP}+a}h^{r+s} \ mod \ p$. Then the user checks the digital signature of the data consumer. If this signature is correct, $com_{DC\_BLINDED}(k_{DC})$ belongs to this data consumer. To verify that this data consumer used this blinded commitment in the *Tag* protocol, the user checks if this blinded commitment 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.

If the service provider cannot show that this commitment is false and the digital signature is valid, this service provider has disclosed the found personal data. If either $com_{DC}(k_{DC})$ or the digital signature of the data consumer is invalid, the data provider in the last disclosure has created an invalid digital watermark by using other values than those gotten from the data consumer in the *Tag* protocol.

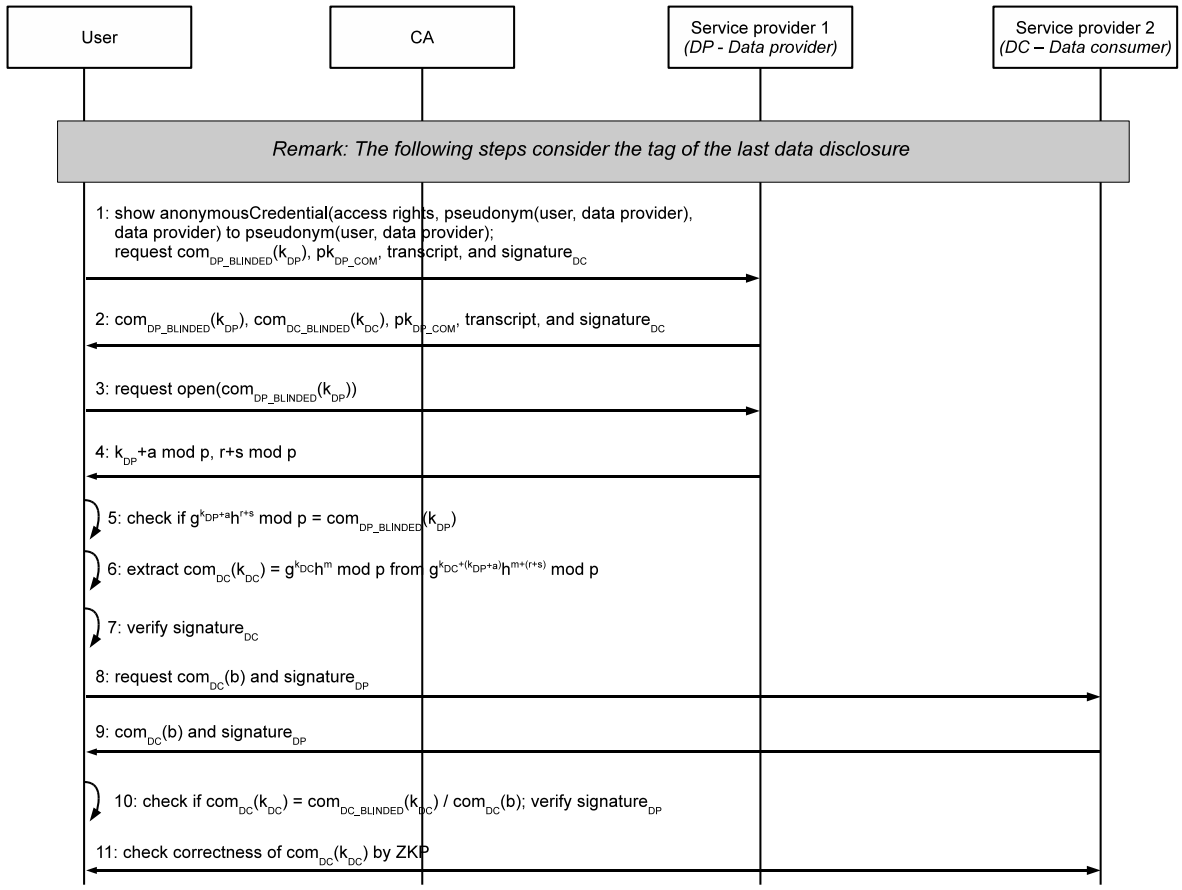

FIGURE 4. Phases E and F of the DETECTIVE *Verify* protocol

6. **Properties of the DETECTIVE Protocols.** We have to show that the DETECTIVE protocols fulfill the defined properties of completeness and soundness. We assume that the digital watermarking algorithm is robust against modification of the data d.

6.1. **Completeness.** We assume that a dishonest service provider has disclosed the user's personal data d further without adding the new data provenance information by means of a digital watermark for the upcoming disclosure, i.e., this service provider has not run the *Verify* protocol. In the scenario of 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 personal data d (shooting an x-ray image), this service provider has an incentive to follow the *Verify* protocol. Hence, the homeland clinic has given correct values to the protocol and has proven the correctness of the next data consumer's digital signature regarding the data consumer's cryptographic commitment $com_{DC\_BLINDED}(k_{DC})$.

In a run of the *Verify* protocol, the data consumer has to show the relationship between $com_{DC\_BLINDED}(k_{DC})$ and the master identity k_{DC}. This checks involves the check of the data consumer's digital signature ($signature_{DC}$) and of the commitment $com_{DC}(k_{DC})$. The user has gotten $signature_{DC}$ from the data provider and can check it with the public key of the data consumer. The user knows this data consumer due to the corresponding delegated access right to this consumer. If the data consumer's digital signature is valid, then it is assured that $com_{DC\_BLINDED}(k_{DC})$ belong to the data consumer under investigation. Next the user has to check the relationship of $com_{DC\_BLINDED}(k_{DC})$ to the data consumer's identity k_{DC}. After unblinding the commitment $com_{DC\_BLINDED}(k_{DC})$, this

check is done by means of a zero-knowledge proof. Because of the soundness property of zero-knowledge proofs, the proving party, i.e, the data consumer, cannot cheat in a zero-knowledge proof [16]. If the digital signature of the data consumer and the cryptographic commitment of the data consumer are correct and $com_{DC\_BLINDED}(k_{DC})$ is part of the last digital watermark of d, then this is an evidence that the data provider (in the example the data center provider) has disclosed d to this non-authorized data consumer (in the example the pharmaceutical company). Otherwise the user runs the phases E and F of the *Verify* protocol for the next 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 data consumer (the clinic abroad) has disclosed d (the patients x-ray image) to the pharmaceutical company.

6.2. **Soundness.** We assume that both service providers involved in the disclosure of d have violated the agreed-upon obligations with the user and disclosed the users personal data d. They aim to conceal their identities as the data provider in this disclosure 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 know the watermarking key. Regarding the attack (a), if the one acting as the data provider wants to conceal that he has disclosed personal data to a non-authorized service provider, 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 recursively in the disclosure chain until the first data consumer, the user can detect the dishonest behavior of the first data consumer. The reason is that the user 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 anonymous credential. Also, this service provider has proven to the first data provider that his commitment refers to k_{DC}. This forces the first data provider to follow the *Verify* protocol. Therefore, at least the second service provider of the disclosure chain is dishonest.

Regarding the attack (b), the data center provider or the clinic abroad could have disclosed d to the pharmaceutical company. If the clinic abroad 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 data center provider, then this provider will be identified as the violator due to the digital watermark for the disclosure of d from the homeland clinic to the data center provider and because of the completeness property.

Concerning the attack (c), the data provider or consumer has used a cryptographic commitment, which does not correspond to their secret key. The cheater must be able to show the knowledge of the committed value. Since a commitment relates to another value than k_{DC} or k_{DP}, the cheating party either cannot convince the user 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 user would identify the data provider as the violator since the data consumer cannot prove the knowledge of k_{DC} to the commitment $com_{DC}(k_{DC})$. Even if the data provider has used a commitment different to k_{DP} but he knows the committed value, then he can still show his role as the data provider. But if he has not used this commitment in the *Tag* protocol, then it is not part of the digital watermark and the user cannot extract the

correct commitment $com_{DC}(k_{DC})$ of the data consumer. 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.

7. **Outlook.** Today, privacy in cloud computing is 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. We have shown a privacy risk regarding the usage abroad of electronic health records. Our proposal of usage control through data provenance enables users to check ex post whether software service providers are actually obeying and enforcing the agreed-upon privacy rule. 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 the user as well as remaining the x-ray image usable for the medical institutions.

Acknowledgement. This work was funded within the postdoctoral scholarship program *Forschung an internationalen Wisenschafts- und Technologiezentren (FIT)* of 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). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the article.

REFERENCES

[1] 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, p. 31–50, 1995.

[2] U.S. Department of Health & Human Services, Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, http://www.cms.hhs.gov/HIPAAGenInfo, 1996.

[3] M. Hilty, D. Basin, and A. Pretschner, On obligations, *Proc. of the ESORICS 2005*, Springer, vol. 3679, pp. 98–117, 2005.

[4] S. Sackmann, J. Strüker, and R. Accorsi, Personalization in Privacy-Aware Highly Dynamic Systems, *Communications of the ACM 49(9)*, ACM Press, pp. 32–38, 2006.

[5] S. Wohlgemuth and G. Müller, Privacy with Delegation of Rights by Identity Management, *Proc. of ETRICS 2006*, Springer, vol. 3995, pp. 75–190, 2006.

[6] T.K. Dang, Security protocols for outsourcing database services, *Information & Security-An International Journal*, ProCon, vol. 18, p. 85–198, 2006.

[7] A. Pretschner, M. Hilty, F. Schütz, and C. Schaefer, Usage Control Enforcement: Present and Future, *IEEE Security & Privacy 6(1)*,Proceeding of IEEE, pp. 44–53, 2008.

[8] G. Karjoth, M. Schunter, and M. Waidner, Privacy-enabled Services for Enterprises, *Proc. of the 13th International Workshop on Database and Expert Systems Applications, IEEE Computer Society*, pp. 483–487, 2002.

[9] H. Mantel, Information Flow Control and Applications-Bridging a Gap, *Proc. of FME 2001*, Springer, vol. 2021, pp. 153–172, 2001.

[10] M. Casassa Mont, and S. Pearson, An Adaptive Privacy Management System for Data Repositories, *Proc. of TrustBus 2005*, Springer, vol. 3592, pp. 236–245, 2005.

[11] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2008.

[12] B. Pfitzmann and M. Schunter, Asymmetric Fingerprinting, *Proc. of EUROCRYPT 1996*, Springer, vol. 1070, pp. 84–95, 1996.

[13] M. Li, R. Poovendran, and S. Narayanan, Protecting patient privacy against unauthorized release of medical images in a group communication environment, *Computerized Medical Imaging and Graphics*, Elsevier, vol. 29, pp. 367–383, 2005.

[14] J. Camenisch, and E. Van Herreweghen, Design and Implementation of the idemix Anonymous Credential System, *Proc. of the 9th ACM Conference on Computer and Communications Security*, ACM Press, pp. 21–30, 2002.

[15] D. Chaum, J.-H. Evertse, and J. van de Graaf, An improved protocol for demonstrating possession of discrete logarithms and some generalizations; *Proc, of EUROCRYPT 1988*, Springer, vol. 304, pp. 127–141; 1988.

[16] S. Goldwasser, S. Micali, and C. Rackoff, The knowledge complexity of interactive proof systems, *SIAM J. Computation* 18(1), pp.186–208, 1989.