Revocable Anonymity

Stefan Köpsell[1], Rolf Wendolsky[2], and Hannes Federrath[2]

[1] Dresden University of Technology
sk13@inf.tu-dresden.de
[2] University of Regensburg
{rolf.wendolsky, hannes.federrath}@wiwi.uni-regensburg.de

Abstract. Anonymity services in the EU may be forced by the new EU data retention directive to collect connection data and deanonymise some of their users in case of serious crimes. For this purpose, we propose a new privacy-friendly solution for incorporating revocation in an anonymous communication system. In contrast to other known methods, our scheme does not reveal the identity of a user to any other entity involved in the revocation procedure but the law enforcement agency. Another advantage is, that no user will need to provide more identifying information than his connection (IP) address, that is what he needs to communicate with the system anyway. The proposed scheme is based mainly on threshold group signatures and threshold atomic proxy re-encryption.

1 Introduction

On december 14, 2005, the EU parliament has passed a data retention directive that forces all EU telecommunication providers to store the connection data of their users for at least six months. The goal is to use the data "for the prevention, investigation, detection and prosecution of serious criminal offences" [EP05]. Unfortunately, this act gives the member states' legislature the possibility, almost at its will, to raise the retention interval and to define the type of crimes that allow the local law enforcement agencies to request the connection data.

If running in the EU, even anonymity services are forced to obey the act mentioned, and non-EU countries will adapt to this directive with a high possibility, too. In Germany, for example, even without this new law anonymity providers are, in certain cases, obliged to release connection data to law enforcement agencies [FeGo04]. Therefore, sooner or later, a deanonymisation protocol is needed for all anonymity systems that are not of pure theoretical nature.

In this paper we propose a new scheme that - in case of a court order - allows for deanonymisation without weakening the general trust model of an anonymity service. Moreover, the revocation of anonymity should preserve the privacy of all lawful users, especially without the need of logging all communication data.

The paper is structured as follows: In the next section we describe our requirements for revocation and deduce the general attributes of our scheme. Section 3 gives an overview of related work. Section 4 describes the basic idea and recalls properties of cryptographic primitives used. Section 5 describes our scheme in detail and Section 6 analyses the security of the scheme.

G. Müller (Ed.): ETRICS 2006, LNCS 3995, pp. 206–220, 2006.

2 Revocation Requirements

The scenario we have in mind is pictured in Figure 1. Some users want to access the Internet anonymously and therefore use an anonymity service C. This service is based on n intermediary servers. We will call such a server *Anonymiser*.

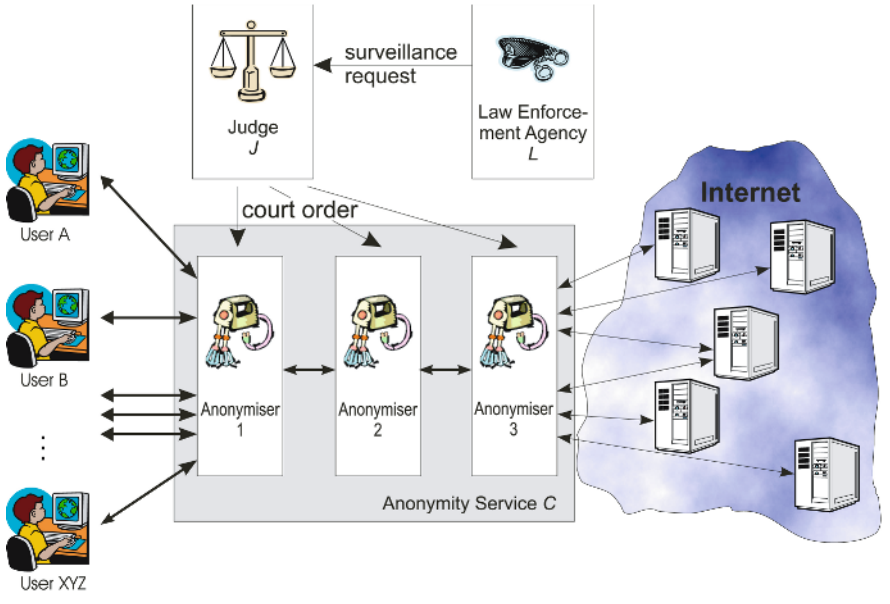

Fig. 1. Anonymous communication system

As the revocation scheme should not depend on a certain anonymity mechanism it does not matter how the anonymity service works in detail. In practice the anonymity service could be based on Mix cascades [Chau81], DC-nets [Chau88], threshold-mixes [Jak99a] etc.

The only assumption on the type of service is that the service offers unconditional anonymity as long as not at least k of the n servers collude (e.g. k=n for Mixes). Note that this assumption defines the trust model of the anonymity service: a user has to trust that the number of colluding servers is less than k. Otherwise the service will not provide any anonymity at all.

To depict law enforcement processes, two extra parties are added to the basic system: A law enforcement agency L that wants to observe certain communication relations, and a judge J that may confirm this request by a court order O. If this order is obligatory for the operators of all Anonymisers, the supervision has to be done.

We want to stress these facts, as it turns out that many people have some "back-doored" system in mind if they think about revocable anonymous communication. The term "back-doored" is misleading for various reasons:

- It suggests the existence of a hidden and undocumented functionality within the system – our approach, in contrast, is well documented and especially communicated to the users of the anonymity service.
- It suggests that a single centralised entity has the possibility to deanonymise every arbitrary communication – in contrast, the approach described in this paper needs the cooperation of different entities to deanonymise a certain communication relation. In addition, only a well defined subset of these entities will learn something about the identity of the communication partners.
- It implies that there is an automatic procedure that allows deanonymisation without human interaction. Although the proposed protocol may work in this way, too, our suggestion is that only human representatives of the organisations that run the Anonymisers may trigger "deanonymisation events" (see chapter 6).[1]
- It implies that there exists a "no-back-doored" system for anonymous communication which offers unconditional anonymity. But to our knowledge such a system neither exists in theory nor in practice – due to the fact that deanonymisation is always possible if more or stronger parties than specified by the attacker model collude.

Figure 2 illustrates that designs for revocable anonymity are not only black or white solutions regarding privacy, but exist in different shapes of grey:

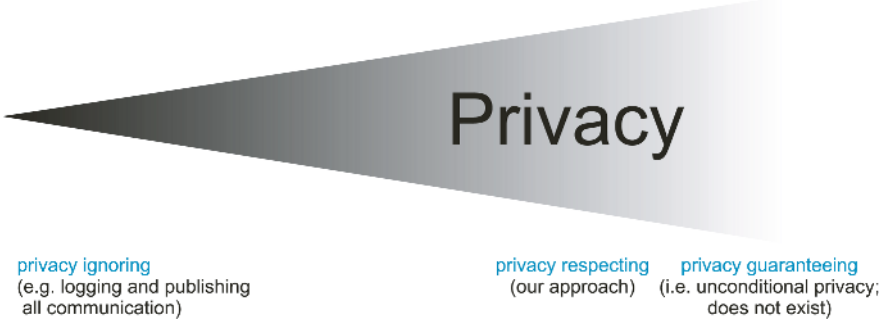

Fig. 2. Designs for revocable anonymity exist in different shapes of grey

As we know from a practical system, law enforcement agencies do typically not observe certain users, but usually just want to know the IP address of the sender of a certain message [KöMi05]. The IP address contains information regarding the ISP, who will, after a court order, provide the law enforcement agency with the name, address etc. of the corresponding user. Therefore, the proposed scheme is desinged to reveal the connection data of an observed user request only, but may of course be easily extended to provide more identifying information.

[1] In the following it is assumed that each Anonymiser is run by an independent organisation. Therefore "Anonymiser" is used as synonym for "organisation", too.

In the following, the messages requested by L are called "suspicious". The decision which messages are "suspicious" is either based on the recipient's address (IP-address, URL etc.) or on the message content. The procedure how to identify "suspicious" messages is independent of the deanonymisation protocol and is beyond the scope of this paper.

The following requirements summarise the required attributes *Full Traceability* (1,2,3) and *Full Anonymity* (4,5):

1. It has to be feasible to disclose the identity of the sender of any given "suspicious" message. There must be no need to rely on the help of the sender.
2. Revocation should only deanonymise a single user *ID*, but should not affect the anonymity of other users (besides that the size of the anonymity set decreases by one).
3. Based on the link between a user *ID* and a requested "suspicious" message, it must be impossible for any entity (the user itself or entities involved in the revocation process) to lie on the *ID*.
4. For privacy reasons, the link between the *ID* and the "suspicious" message must not be revealed to any other entity than L. In particular, the Anonymisers must not learn anything about *ID*.
5. The revocation scheme has to be compatible with the trust model of the anonymity service, that means at least k of the n Anonymisers have to cooperate to deanonymise a certain user and less than k of them are malicious.

3 Related Work

[Golle04] describes a method for Mix networks that allows a Mix to prove that he is not the sender of a given "suspicious" message. The procedure is based on blind signatures and does not offer the possibility to identify the real sender of the "suspicious" message.

The ticket-based authentication system described in [BeFK01] is also based on blind signatures. Its goal is to protect against flooding attacks. A user has to pseudonymously register with all Mixes and gets so-called tickets (credentials) valid for a short period of time and allowing him to anonymously send messages. The user has to send a valid ticket with every message.

This original method does not offer the option to link a certain message to its sender by means of the tickets. [ClDí03] is an extension of [BeFK01] where this linkage is possible. This is achieved by using fair blind signatures instead of blind signatures. From a privacy point of view a disadvantage of [ClDí03] is, that besides the law enforcement agency also other entities involved in the revocation procedure learn the identity of the sender. Another disadvantage is, that the user needs to request a new ticket for every message he wants to send.

[BaNe99] explains how payment for an anonymity service could be done by the means of anonymous digital cash. The main idea is that every message contains a digital coin which the Mix will get for processing the message. If we used a

fair anonymous digital cash system, then the fairness property could be used to reveal the spender (sender) of the digital coin. But as there are no such payment schemes in practice this does not solve the problem.

4 Preliminaries: Basic Idea and Cryptographic Primitives

The basic idea of our revocation scheme is similar to the one proposed in [ClDí03]: Any request (message) that should reach its recipient has to be signed pseudonymously. A verifier V sitting between the last Anonymiser and the recipients will check this. V will drop any unsigned message. If V detects a "suspicious" request, he demands the disclosure of the true identity of the pseudonym.

Note that this scheme allows sending of revocable and unconditional anonymous messages using the same anonymity service at the same time without changing the anonymity protocol etc. This is achieved by instructing V not to check any signature if the request is for certain recipients (for instance a voting machine), which are allowed to receive anonymous requests unconditionally.

Cryptographic Primitives

In order to explain our solution in detail, we first recall properties of the cryptographic primitives used in the revocation scheme.[2] These building blocks are: *threshold group signatures*, *blind signatures* and *threshold atomic proxy re-encryption*.

Recall the following properties of a threshold group signature scheme that provides *Full Anonymity* and *Full Traceability* [CaGJ99, CaGr04, CaLy04]:

- *Full Anonymity* allows group members to anonymously sign messages. Anyone who knows the public group key can check signatures done by a group member but cannot link a signature to the group member by whom it was created.
- To join the group, a user creates a pseudonym Y and performs the Join(Y) operation with the help of *GM*. As a result, the user learns his secret group key sk_Y and may now forge signatures that are verifyable with the public group key.
- *Full Traceability* means that without the secret key of a group member it is infeasible to create a valid signature that could be linked to this member. Note that this holds even if the secret key of *GM* is exposed, so that *GM* in particular cannot generate signatures that are linkable to this group member.
- The group manager *GM* can revoke the anonymity of a given signature. This will reveal the pseudonym Y under which the signer is known to the group manager.[3]

[2] A security discussion of these primitives is beyond the scope of this paper. They are used as basic building blocks only.

[3] Note that *GM* does not necessarily get to know the true identity *ID* of Y and that the anonymity revocation capability could be separated from the member management capability.

– *Threshold* means that the group manager GM is distributed on n parties and that at least k of these parties are needed to revoke the anonymity of a group member.

Recall the following properties of a blind signature scheme [CaKW04] that provides *Unforgeability* and a *Partial Message Proof* [Rab78]:

– $\mathrm{Sig}_E(m)$ denotes a signature on m done by the entity E.
– *Blindness* allows a user U to get a signature $\mathrm{Sig}_E(m)$ on a message m from a signer E by interacting with E, whereas E does not know the message content and is not able to link $\mathrm{Sig}_E(m)$ with the protocol session during which $\mathrm{Sig}_E(m)$ was created, or with the user that sent the message and received the signature, respective.
– *Unforgeability* means that after k runs of the protocol with the signer, the user cannot obtain strictly more than k valid message-signature pairs.
– $[m]$ denotes a blinded version of m.
– $\mathrm{Sig}_E^{\mathrm{blind}}([m])$ denotes a blind signature on m which after unblinding leads to $\mathrm{Sig}_E(m)$.
– *Partial Message Proof* means that the signer E only signs a message m blindly if he can previously verify a part p_m of the message m. This could be achieved using cut-and-choose protocols or by selecting a blind signature scheme that incorporates zero-knowledge proofs on p_m. In a (simple) cut-and-choose protocol, for example, U sends many blinded versions of the message m that must all contain a valid p_m to E. E selects all but one of them which U has to unblind so that E can read them. E signs the remaining blinded message m if all unblinded messages contain a valid p_m.

Recall the following properties of a threshold atomic proxy re-encryption scheme [Jak99b]:

– A (k, n)-threshold atomic proxy re-encryption scheme allows any k members of a group of n entities to re-encrypt an encrypted message m which is encrypted with the public key of the group. The result of the re-encryption is the message m encrypted with another public key, whereas m is not revealed.
– $\mathrm{Enc}_y(m)$ denotes an encryption of m done with the public key y.
– $\mathrm{Enc}_{y_1}(m) \underset{\mathrm{P}}{\rightarrow} \mathrm{Enc}_{y_2}(m)$ denotes a re-encryption from the public key y_1 to the public key y_2. This will lead to a proof P, showing that both encryptions decrypt to the same message m. Any third party can verify this proof.

5 The Revocation Scheme

This section describes the revocation scheme in detail. We revise our basic idea introducing some new parties and describe the different protocol steps in detail.

The pseudonymous signatures mentioned in the basic idea are in fact group signatures. If V detects a "suspicious" message, the group manager GM will revoke the anonymity of the signature. This leads to the pseudonym Y and a

certificate issued by a third party I. This certificate links Y to an encrypted identity $\mathrm{Enc}_{y_C}(ID)$. This encryption is done with the public key y_C of the anonymity service. The Anonymisers will jointly proxy re-encrypt ID to the public key y_L of the law enforcement agency $L : \mathrm{Enc}_{y_C}(ID) \underset{\mathrm{P}}{\rightarrow} \mathrm{Enc}_{y_L}(ID)$. L can finally decrypt this to ID. Figure 3 illustrates this.

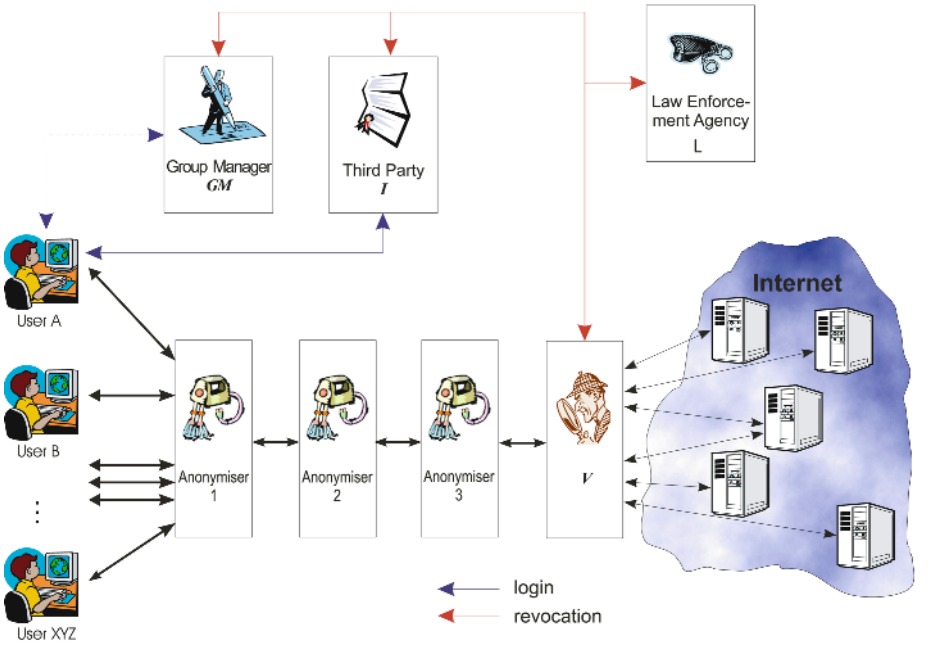

Fig. 3. Overview of the revocation scheme and the involved parties

General Setup

The Anonymisers $A_1, \ldots, A_n$ jointly generate a public key y_C of a (k, n)-threshold atomic proxy re-encryption scheme and the public group verification key y_{GM} of a (k, n)-threshold group signature scheme. They are thus commonly seen as the group manger GM.[4] The party I publishes the public verification key y_I of its blind signature scheme.

User Login Procedure

In order to use the anonymity service each user has to login to it first. Besides the necessary key exchange to encrypt a message according to the Anonymiser protocol, the login procedure comprises the following steps:

1. A user U creates a self-signed certificate that includes his current connection address ID as attribute (e.g. his IP address).

[4] For simplification, the group manager will be seen as separate entity in most cases.

2. He non-anonymously connects to the Anonymiser that may grant access to the anonymity service to let his certificate get signed by him. The certificate will get a timestamp and may only be used for requesting a group signature key as long as the connection to the access-granting Anonymiser is held.[5]
3. U selects a random pseudonym Y.
4. Now the user U contacts the third party I and requests a blind signature $c = (Y, \mathrm{Enc}_{y_C}(ID, \mathrm{Sig}_{ID}(Y, ID)))$
   $U \longrightarrow I : [c], \mathrm{Sig}_{ID}([c])$
5. I issues the blind signature, but only if I is confident that she really signs an encryption of the right ID with respect to U (partial message proof). If this is done by cut-and-choose, U has to reveal Y and $\mathrm{Sig}_{ID}(Y, ID)$ several times so that I can do the encryption $\mathrm{Enc}_{y_C}(ID, \mathrm{Sig}_{ID}(Y, ID))$ to verify the unblinded messages. Therefore, for each blinded message, U has to choose another pseudonym Y_i and re-encrypt $\mathrm{Enc}_{y_C}(ID, \mathrm{Sig}_{ID}(Y_i, ID))$. Otherwise I would know Y and the encrpytion of the corresponding $\mathrm{Sig}_{ID}(Y, ID)$ and could, in collusion with one of the other parties, get the ID of the sender of a malicious message m.
   $I \longrightarrow U : \mathrm{Sig}_I^{\mathrm{blind}}([c])$
6. U unblinds the signature and gets $cert = \mathrm{Sig}_I(Y, \mathrm{Enc}_{y_C}(ID, \mathrm{Sig}_{ID}(Y, ID)))$
7. U becomes a group member by performing the Join() operation with the group manager using the pseudonym Y. U also sends $cert$ to GM. Note that all communication with GM is done unconditional anonymously using the anonymity service C. Otherwise he would get the connection address and therefore, in the end, the real identity of U.
   $U \longrightarrow GM : \mathrm{Join}(Y), cert$
8. Now the user may connect to the anonymiser service using his group signature key for authentication.

Sending Messages Anonymously

U can now send messages anonymously according to the Anonymiser protocol. The additional step he has to do is to sign the messages with his secret group signature key sgk_Y. V will check for every message whether it is signed and verifies the signature with y_{GM}. If the signature is OK and the message is "good", it will be forwarded to the requested resource. If m does not have a valid signature, the message is dropped.

Revoking Anonymity

The prerequisite for revoking anonymity is that V gets a court order O. O contains a public key y_L of the law enforcement agency L and a relation R, which says for every message m if m is "suspicious" or "good"; $R : \{m\} \rightarrow \{$"good", "suspicious"$\}$.

[5] Note that this temporary certificate may be replaced by a real one if a PKI with trusted authorities exists. This certificate could contain much more information than only the connection address at a certain time and would therefore tend to be less privacy-friendly but far more accountable.

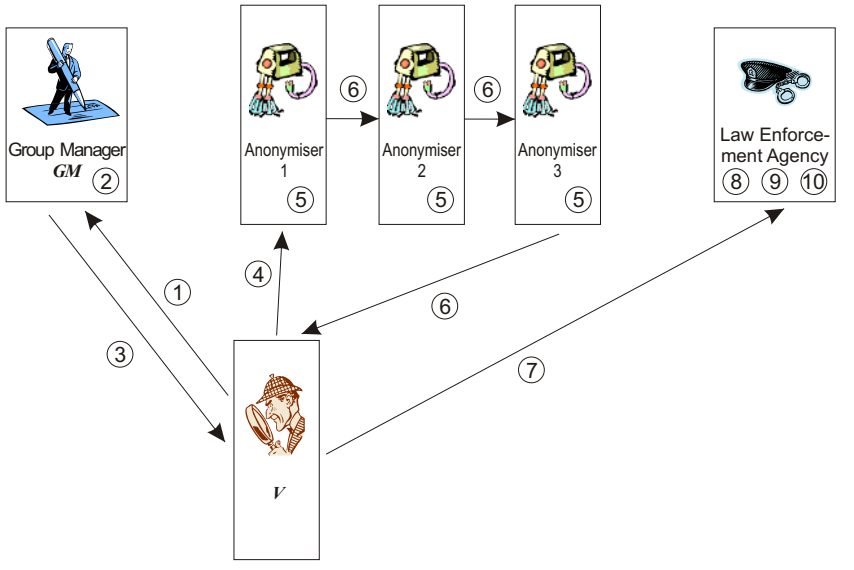

Fig. 4. The revocation procedure

If V detects a "suspicious" message m, revealing the identity of the sender works as follows (cf. Fig. 4):[6]

1. V shows m, $\mathrm{Sig}(m)$ and O to GM.
2. GM checks that $R(m) =$ "suspicious" and verifies $\mathrm{Sig}(m)$.
3. GM reveals $cert = \mathrm{Sig}_I\,(Y, \mathrm{Enc}_{y_C}\,(ID, \mathrm{Sig}_{ID}(Y, ID)))$ and a proof Pr that $\mathrm{Sig}(m)$ was done by Y.
4. V verifies $cert$ and Pr and shows m, $\mathrm{Sig}(m)$, O, $cert$ and Pr to k of the Anonymisers $A_1, \ldots, A_n$.
5. Each Anonymiser A_i of these k Anonymisers checks that $R(m) =$ "suspicious" and verifies $\mathrm{Sig}(m)$, $cert$ and Pr.
6. The k Anonymisers jointly proxy re-encrypt $\mathrm{Enc}_{y_C}\,(ID, \mathrm{Sig}_{ID}(Y, ID))$:
   $\mathrm{Enc}_{y_C}\,(ID, \mathrm{Sig}_{ID}(Y, ID)) \underset{\mathrm{P}}{\rightarrow} \mathrm{Enc}_{y_L}\,(ID, \mathrm{Sig}_{ID}(Y, ID))$
   One of the k Anonymisers sends $\mathrm{Enc}_{y_L}\,(ID, \mathrm{Sig}_{ID}(Y, ID))$ and the proof P that both encryptions decrypt to same content to V.
7. V verifies P and sends m, $\mathrm{Sig}(m)$, $cert$, Pr, $\mathrm{Enc}_{y_L}\,(ID, \mathrm{Sig}_{ID}(Y, ID))$ and P to L.
8. L checks that $R(m) =$ "suspicious" and verifies $\mathrm{Sig}(m)$, $cert$, Pr and P.
9. L decrypts $\mathrm{Enc}_{y_L}\,(ID, \mathrm{Sig}_{ID}(Y, ID))$ to ID and $\mathrm{Sig}_{ID}(Y, ID)$.
10. L verifies $\mathrm{Sig}_{ID}(Y, ID)$.

[6] We assume that every non malicious party will only proceed if the checks she has to do are successful.

Efficiency Remarks
In practical systems performance is crucial. Especially when no revocation takes place - that is the case most of the time the system is running - the performance of the underlying anonymity service should be affected as little as possible.

The overhead introduced arises from the group signature check that V has to perform for every message. In case the scheme described in [CaGr04] is used, the verification of a single signature takes about three times as long as the verification of an RSA signature with comparable security parameters. If the anonymity service introduces linkability between messages by the means of anonymous communication *channels*, then V only needs to check one signature per channel instead of one per message. Additionally, if the anonymity service concurrently outputs a bunch of messages, a group signature scheme should be used where verifying x messages at once is less expensive than verifying x times a single message [BeGR98]. This is appropriate for instance for anonymity services based on Mixes working in batch mode.

6 Security Analysis

As defined in section 2, the revocation scheme should provide the two properties *Full Traceability* and *Anonymity*:

1. *Full Traceability* means that without the secret key of a user it is infeasible to create a valid revocation that wrongly leads to this user (or more informally: it is impossible for a given message m sent by the user ID to convince L that m was sent by another user ID'.)
2. *Anonymity* means that without the help of k colluding Anonymisers or all but one users it should hold that:
   - **A1** besides L and the sender U no other party learns the identity ID of the sender U of a given "suspicious" message m
   - **A2** in case no revocation takes place the system should provide the same anonymity as the underlying anonymity service would provide without the revocation scheme. Informally that means that the existence of the revocation scheme does not influence the anonymity of "good" messages.

Full Traceability
This property deduces from the properties of the chosen signature schemes. In order to analyse if the proposed scheme offers *Full Traceability*, we have to look at steps 2 and 8 of the login procedure and at the checks done by L in the steps 8 and 10 of the revocation procedure.

(1) In step 8 of the login procedure, the user U has to authenticate himself at the anonymity service with his group signature key that, in the end, leads to his current connection address (identity) ID. If the user does not collude with the Anonymiser that grants access to the service or with the third party I, he has no chance to cheat by presenting another certificate or by choosing another address, as the Anonymiser has signed the certificate in step 2, both can compare the ID attribute and the user's current address, and the blind and group signature keys are replaced within short time periods.

(2) If U colludes with the Anonymiser that grants access, he may lie on his real address. But without this protocol, and if all connection addresses simply had to be logged and given to the law enforcement agency instead (worst case for privacy), the problem would be the same if these parties colluded. This is therefore no weakness of the revocation protocol[7].
(3) In step 10 L verifies the signature $\mathrm{Sig}_{ID}(Y, ID)$, which in fact is a statement given by the user with ID that he is responsible for all messages signed by the pseudonym Y. As the signature scheme itself complies with unforgeability, it is impossible for an attacker to generate a signature $\mathrm{Sig}_{ID'}(Y, ID')$ without the help of ID'.
(4) In step 8 L verifies $\mathrm{Sig}_Y(m)$ and Pr, where Pr is a proof that $\mathrm{Sig}_Y(m)$ was done by Y. This is in fact a check that GM has revealed the right Y. Due to the *Full Traceability* property of the group signature scheme, an attacker could not create a valid signature that frames Y without knowing the secret key of Y. Note that this holds even if the group manager colludes with the attacker.

As shown in (1), (3) and (4) the attacker can neither manipulate $\mathrm{Sig}_Y(m)$ nor $\mathrm{Sig}_{ID}(Y, ID)$. Therefore m has to be sent by ID. In case of (2), the manipulation is not in the scope of this scheme, but of the law enforcement agencies and the attacking Anonymiser that will be punished if caught.

Anonymity
Note that, according to the assumptions made in section 2, regardless of the revocation scheme the anonymity service will not provide any anonymity if at least k Anonymisers collude.

(1) A1 and A2 hold as long as the group manager does not collude with the attacker. This derives from the facts that
  – the GM is the only one that can reveal the pseudonym of a given sender that is needed to get his ID (satisfies A1) and
  – the only change made to the underlying anonymity service was adding a group signature and this scheme offers full-anonymity (satisfies A2).
(2) In order to break A1, the attacker has to learn the true identity ID of the owner of Y. GM himself does not know ID because during the Join() operation (step 7 of the login procedure) the communication with the user was done by means of an unconditional anonymity service. Also colluding with I would not help, because the linkage between Y and ID by means of the signature issued by I on *cert* is impossible due to the blindness property of the signature scheme.
(3) If it is possible for the attacker to reveal the pseudonym Y of the sender of a given message m, A2 would be broken as the attacker could link messages which are sent by the same sender and therefore has at least a higher chance of intersection attacks. But as less than k Anonymisers collude with the attacker, GM cannot reveal Y.

[7] If a PKI with trusted authorities is available, these temporary certificates may be replaced by real ones with high accountability but less privacy-friendliness.

This makes clear that the anonymity of the system is not tampered by this scheme apart from the fact that, of course, the anonymity set is decreased by one member for each "suspicious" message.[8]

Additional Remarks

It is not possible to simplify the revocation scheme by omitting the blind signature from party I and just using the identity ID of U as pseudonym Y for the threshold group signature scheme. This would mean that, in the revocation process, all k revoking group managers or Anonymisers, respective, would learn both ID and m and may easily link them. The benefit of the revocation scheme would be at least very questionable, and virtually no benefit would remain if $k = n$.

If V is "malicious" with respect to the law enforcement agency L, he could ignore and, in order not to make himself "suspicious", block all "suspicious" messages. In this case, no revocation is done at all. This behaviour of V is not preventable in general, but could be detected later on if m is not blocked and leads to an incident detectable by L. Otherwise, if a revocation takes place, the procedure either reveals the identity of the sender of the "suspicious" message or identifies a malicious party (V, GM, I, A_i).

Identifying Malicious Parties

If V tries to revoke the anonymity of a "good" message m, he has to prove that he has shown m, $\mathrm{Sig}(m)$ and O to GM. As V is not able to do this, he is detected as malicious party and the revocation procedure fails.

If the user U colludes with I and uses a faked ID certificate, I would get exposed as malicious party as the ID certificate has to be signed by the access-granting Anonymiser[9] and the timestamp in the certificate would not fit to the validity of the blind signature key of I.

If GM can't reveal the pseudonym Y of the group member who signed m or can't show a valid $cert$ then GM is malicious. If the proof Pr does not hold then some Anonymisers cheat during the re-encryption. The re-encryption scheme reveals which Anonymisers are malicious. If L can't decrypt what he gets to a valid signature $\mathrm{Sig}_{ID}(Y, ID)$ then I is malicious.

Recommendations for Combining Entities

The revocation scheme introduces a lot of new entities: I, J, V, L, and GM. The security discussion has made clear that a collusion between these entities does not lead to the deanonymisation of a message m without the help of at least k Anonymisers or will at least expose the malicious parties. It is therefore allowed to simplify the organisational structure and combine these entities among each other and with the Anonymisers. These combinations may influence the general performance of the protocol and, in a small manner, security and trust aspects.

[8] Even this is not the case for more than one "suspicious" messages that are sent by the same sender.

[9] Note again that these temporary certificates may be replaced by real ones.

Generally, the more entities are combined, the more trust must be set in single entities by the system users.

Combining J with other entities does not make sense, as, in this context, judges won't do any other work than creating court orders for L and, on the other hand, must be independent from other entities by law.

I could be integrated in all Anonymisers that grant access to the anonymity service, for example in the first Mix of a Mix cascade. The creation of the temporary certificate may be thus combined with the creation of the blind signature.

V may be operated by L. This would mean that all "suspicious" messages that are not blocked by the last Anonymiser will surely be deanonymised. On the other hand, overeager officers could try to block some "good" messages. Therefore, a better choice would be to let the last Anonymiser in the cascade run V, as he has the power to block (and thus hide) messages anyway.

For the reason that an Anonymiser run by a police authority will diminish the general user trust in the whole service greatly, L should never be combined with an Anonymiser. Even if combined with V, it may be realised by the users as part of the system. Combining it with another entity does not make sense, either, as law enforcement agencies won't do any work that is not directly useful for crime detection, prevention and prosecution.

Last but not least GM is, as defined before, integrated in the n Anonymisers.

7 Conclusion

We have proposed a new scheme for incorporating revocation in an anonymous communication system. In contrast to known methods, our scheme is zero-knowledge with respect to any entity involved in the revocation procedure but the law enforcement agency. Another advantage is, that the user needs to authenticate himself only once to anonymously send as many messages as he wants. Moreover, the very privacy-friendly user identification by his connection address may be sufficient for his authentication, as the responsibility to find the real identity behind the address may be assigned to the law enforcement agency.

This scheme is sufficient to serve the type of surveillance requests currently launched by law enforcement agencies, namely to revoke the anonymity of the sender of a certain request. A subsequent work could be to design schemes that allow for the uncovering of all requests of a certain user, while diminishing the privacy of the other anonymity group members as little as possible. As stated before, this kind of revocation is not yet needed in practical systems, but could be of interest in the future.

Acknowledgement

First we wish to thank Julius Mittenzwei who asked the question: "How can revocation be done so that I as a Mix operator could not learn anything about

the sender of a 'suspicious' message?". Thanks also to Jan Camenisch for helping to find and understand the right cryptographic primitives. Moreover, we wish to thank the members of the research group in Dresden, namely Mike Bergmann, Rainer Böhme, Sebastian Clauß, Thomas Kriegelstein, Andreas Pfitzmann, Sandra Steinbrecher and Andreas Westfeld. The discussions with them helped a lot in developing the revocation scheme.

References

[BaNe99] Matthias Baumgart, Heike Neumann: Bezahlen von Mix-Netz-Diensten. Verläßliche IT-Systeme - VIS 1999, Vieweg, 1999.

[BeFK01] Oliver Berthold, Hannes Federrath, Stefan Köpsell: Praktischer Schutz vor Flooding-Angriffen bei Chaumschen Mixen. in: Patrick Horster (Hrsg.): Kommunikationssicherheit im Zeichen des Internet. DuD-Fachbeiträge, Vieweg, 2001, 235–249.

[BeGR98] Mihir Bellare, Juan A. Garay, Tal Rabin: Fast Batch Verification for Modular Exponentiation and Digital Signatures. Advances in Cryptology — EUROCRYPT '98, LNCS 1403, Springer, 1998, 236–250.

[CaGJ99] Ran Canetti, Rosario Gennaro, Stanislaw Jarecki: Adaptive Security for Threshold Cryptosystems. Advances in Cryptology — CRYPTO '99, LNCS 1666, Springer, 1999, 98–115.

[CaGr04] Jan Camenisch, Jens Groth: Group Signatures: Better Efficiency and New Theoretical Aspects. in: Proc. of Security in Communication Networks (SCN 2004), LNCS 3352, Springer, 2004, 120–133.

[CaKW04] Jan Camenisch, Maciej Koprowski, Bogdan Warinschi: Efficient Blind Signatures without Random Oracles. in: Proc. of Security in Communication Networks (SCN 2004), LNCS 3352, Springer, 2004, 134–148.

[CaLy04] Jan Camenisch, Lysyanskaya: Signature Schemes and Anonymous Credentials from Bilinear Maps. Advances in Cryptology — CRYPTO 2004, LNCS 3152, Springer, 2004, 56–72.

[Chau81] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2, 1981, 84–88.

[Chau88] David Chaum: The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1(1), 1988, 65–75.

[ClDí03] Joris Claessens, Claudia Díaz, et al.: APES, Anonymity and Privacy in Electronic Services, Deliverable 10, Technologies for controlled anonymity, 2003, `https://www.cosic.esat.kuleuven.ac.be/apes/docs/APES_d10.pdf`, 34–40.

[EP05] European Parliament: European Parliament legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 C6-0293/2005 2005/0182(COD)), 2005

[FeGo04] Hannes Federrath, Claudia Golembiewski: Speicherung von Nutzungsdaten durch Anonymisierungdienste im Internet. Datenschutz und Datensicherheit DuD 28/8, 2004, 486–490.

[Golle04] Philippe Golle: Reputable Mix Networks. in Proc. of Privacy Enhancing Technologies workshop (PET 2004), 2004, LNCS, Springer

[Jak99a] Markus Jakobsson: Flash mixing. in Proc. of 1999 ACM Symposium on Principles of Distributed Computing (PODC), 1999, 83–89.

[Jak99b] Markus Jakobsson: On Quorum Controlled Asymmetric Proxy Re-encryption. in Proc. of the Second International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1560, Springer, 1999, 112–121.

[KöMi05] Stefan Köpsell, Tobias Miosga: Strafverfolgung trotz Anonymität - Rechtliche Reahmenbedingungen und technische Umsetzung, DuD Datenschutz und Datensicherheit, Heft 7, Vieweg, 2005, 403–409

[Rab78] M. Rabin: Digital signatures. in: Foundations of Secure Computation, R. DeMillo, D. Dobkin, A.Jones and R.Lipton (editors), Academic Press, 1978, 155–168.