ANONYMOUS SOCIAL STAMPS
Authenticating Anonymous Statements to Friends with Privacy

Sandeep S. Kumar
Information and System Security Group, Philips Research Laboratories, Eindhoven, The Netherlands

Keywords: Privacy, Trust, Social network.

Abstract: Numerous online services and applications for smart devices exist today on the internet which claim almost similar functionalities. This inevitably leads to the problem of being able to choose the right one which is mostly done today by trial-and-error. However this gets tricky if it involves sharing privacy sensitive information with the service e.g. in the case of health and well-ness services. A customer's trust in a new online service is known to increase based on testimonials (or observable behavior) of people within a social distance (friends, friends-of-friends etc). Linking testimonials to users requires releasing one's social network information which by itself is privacy invasive. The paper presents the concept of an *anonymous social stamp* which can be assigned to anonymous statements and help prove that the statement was made by a particular member of an external social networking site. Trust can then be derived based on the social distance between the persons concerned: the person who made the statement and the person verifying the statement. A possible implementation of the concept is shown with the existing infrastructure of RSA keys already in use by social networking sites. The concept is applicable for the new services that can create confidence in new users by revealing anonymous data sharing configurations of other users with the service.

1 INTRODUCTION

An incredible amount of choice exists today in web services and applications that can be used online or downloaded onto various smart devices. With this incredible choice comes the problem of determining which of them are useful and actually deliver what they claim. These services and applications can range from simple productivity applications like collaborative text-processing to more advanced applications for health and well-ness like tracking vital bodily signals. Most of these applications require sharing certain amount of privacy sensitive information. This makes it even more important to make an educated decision on which applications to install and how much information to share with such services.

It is well known that people tend to use testimonials and advices provided on various aggregation sites like epinions (Epinions, 2010) while choosing services. The main idea behind such reputation systems (Resnick et al., 2000) is that the majority of the crowd can help filter out scrupulous service providers. However the concern is that such systems are easy to manipulate since ratings are provided by people with no prior trust relationship. Therefore most of these trust and reputation systems (Josang et al., 2007) are faced with the problem of linking pseudonyms to people one can trust. Another concern is that such methods do not help identify services that would best fit to one's individual needs but rather on average to a wider group.

Health and well-ness services is one of the areas that urgently require trusted statements and help in making educated decision of using different applications. Health and well-ness has become a buzzword that is increasingly being used by many fraudulent services to attract new customers. Such services mostly don't work or are sometimes even not safe for some consumers. The increasing numbers of such incidents have even lead the Federal Trade Commission (FTC, 2010a) to set up a dedicated information site for consumers to detect misleading and deceptive health claims at Who Cares (FTC, 2010b). The European Healthcare Fraud and Corruption Network (EHFCN) has recognized that one of the reasons that fraud happens is when providers could have conflicts of interest that affect their judgement (EC, 2010a). Customers that have either experienced or heard/read about these much publicized frauds are very reluctant to use any new heath and well-ness services. There-

S. Kumar S. (2010).
ANONYMOUS SOCIAL STAMPS - Authenticating Anonymous Statements to Friends with Privacy.
In *Proceedings of the International Conference on Security and Cryptography*, pages 183-188
DOI: 10.5220/0002993401830188

fore, creating trust in the new heath and well-ness services would be a very important requirement for new service providers. Additionally, customers need to be confident to share vast amounts of sensor data and private medical information that would be needed to provide the service. Legislation like the Unfair Commercial Practices Directive (Directive 2005/29/EC) (EC, 2010b) can only deter certain amount of misleading claims from service providers but cannot create confidence in the services as being beneficial.

1.1 Our Contribution

Knowledge about the social distance of a new customer with existing consumers of a service is impossible to determine without access to the social network of the new and existing customers. However, this data is readily available at the numerous social networking sites. These social networks have evolved into an important source of communication and trust building on the internet. These trust relationships can either be the individuals trust relationships in the physical world or new ones based on virtual interactions.

For a health and well-ness service provider, creating and administrating yet another social network would not be preferred option but to have a mechanism that allows tapping into the existing information at the social networks to give the assurance of the social distance between two parties. However, revealing a person's static identity at a social networking site or openly revealing one's social network is privacy invasive. Therefore external sites that would like to create trust in their services through recommendations from friend's network, need a mechanism to link into the social networks without invading privacy. The mechanism should provide enough flexibility such that individuals are not forced to reveal their social networks openly if they do not desire. Additionally, the social networking site should not be able to gather and learn about the various external services that the individual subscribes to based on this mechanism.

The main idea of the paper is an *anonymous social stamp* (created using existing RSA key certificates of the social networking sites) that individuals can attach to a statement (reviews, advices, configurations, etc.) on service providers web-site or other review aggregation sites for others to view. A new customer of the service or application can view this statement and if within a social distance can verify it.

The paper is organized as follows, in Section 2 we clearly define the setting and the various parties involved. In Section 3 the security and privacy requirements for our solution is described. Section 4 presents the construction of our anonymous social stamp solution. The various interactions for initialization, generation and verification of the stamp is also presented. In Section 5, we present other useful applications of the anonymous stamp and end with conclusions in Section 6.

2 SCENARIO

As mentioned previously, testimonials and advices to use new services can have additional value if it can be proved that they are written by someone within a social distance like *friends-of-friends*. This would provide some amount of trust in these statements compared to statements made from total strangers. We use a social networking site as a way to determine this social distance. To make clear the setting, we first present the various parties in the system and their roles. Then we discuss the security and privacy requirements for the different parties involved.

2.1 System Model

We present the relevant parties with an example as shown in Figure 1. *Alice* is the party providing an anonymous testimonial (or rating) of a service. However she would like to attach a proof (stamp) that can help others viewing the testimonial to derive some amount of trust in that statement, if they are related within a social distance. *Bob* is a new customer who would like to use the service and make an educated decision based on the testimonials (one of which is from Alice). He retrieves the testimonial and uses the anonymous social stamp to contact the social networking site to know if the anonymous testimonial writer is within a certain social distance of him. Based on this information he can decide to either trust the testimonial or ignore it.

3 SECURITY AND PRIVACY REQUIREMENTS

For the anonymous social stamp to work as shown in the scenario it has to fulfill certain security and privacy requirements as mentioned below:

- **Verifiability.** The social stamp can prove to a verifier (Bob) with the help of the social networking site that the statement indeed belongs to a specific user of the social networking site. The real identity or pseudonym at the social networking site is not revealed but only the social distance is revealed by the social networking site based on the

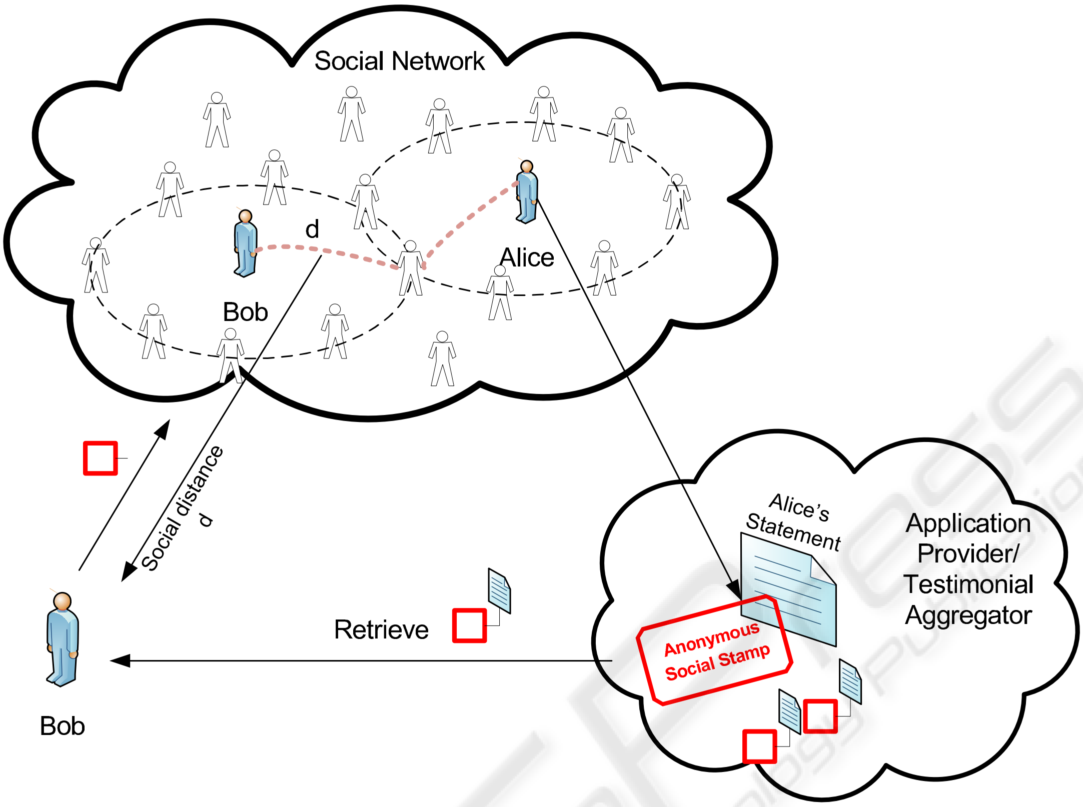

Figure 1: Implementation scenario for the anonymous social stamp.

verifier's (Bob) social distance to the statement creator's (Alice) at the networking site.

- **Secure Binding.** The stamp is publicly visible to everyone and therefore should not be possible to copy to a different pseudonym or statement by anyone.
- **Privacy of the Creator.** The stamp by itself does not reveal the identity of the creator (Alice) to anyone except to the social networking site.
- **Unlinkability of the Creator.** The stamps alone do not enable linking the creator (Alice) across different sites.
- **Privacy of the Verifier.** The verification of the stamp does not require the verifier to show the social networking site the statement or the site from which it was obtained. This is minimize the social networking site from knowing the different services he is interested in.

4 THE ANONYMOUS SOCIAL STAMP

Before we present the technical details of the Anonymous Social Stamp, we first assume the following terminology:

- The external service can be uniquely identified as $\mathfrak{W}$. This could be the unique url or the SSL certificate of the service.
- The statement (review, advice, etc.) to which the social stamp needs to be attached at $\mathfrak{W}$ be represented as $\mathfrak{T}_i$, and uniquely identified by the pair $\mathfrak{T}_i, \mathfrak{W}$. For practical purposes, we assume that the pair $\mathfrak{T}_i, \mathfrak{W}$ can be converted to a single value h using a publicly known hash function, i.e, $h_i = Hash(\mathfrak{T}_i, \mathfrak{W})$.
- The social networking site is represented as $\mathfrak{N}$.
- The user that creates the social stamp (Alice) has the pseudonym $I_{\mathfrak{N}}$ at the social networking site $\mathfrak{N}$. She also has a shared secret $S_{I_{\mathfrak{N}}}$ with social networking site (e.g. a hashed password).
- The verifier's (Bob) identity at the social networking site $\mathfrak{N}$ be $V_{\mathfrak{N}}$.

- The social network $\mathfrak{N}$ possesses the RSA public-private key pair $\{P_\mathfrak{N}, S_\mathfrak{N}\}$. Based on (Rivest et al., 1978), the keys $P_\mathfrak{N}$ and $S_\mathfrak{N}$ exhibits the following property:

$$g^{(P_\mathfrak{N}.S_\mathfrak{N})} \mod n = g \tag{1}$$

for any g and for public n as defined in (Rivest et al., 1978). The method to generate these RSA keys and their properties are well known and will not be described further here. However note that all operations shown further are done $\mod n$ even when not explicitly mentioned.

We now describe how the anonymous social stamp can be created for a statement and verified. Figure 2 shows the various phases from initialization, generation and verification of the stamp. We describe each step in detail and show the correctness of the protocol.

4.1 Initialization Phase

The first step is the initialization phase where the user Alice at the social networking sites is provided with keys to create any number of anonymous social stamps. The social networking site generates a large random g. This g is fixed for each social network and known publicly. Alice who possess the identity $I_\mathfrak{N}$ at the social networking site, is given the two keys $K_\mathfrak{N}$ and $K_{I_\mathfrak{N}}$ derived as follows:

- $K_\mathfrak{N} = g^{P_\mathfrak{N}}$, which is same for all users and need not be kept secret since it is created using a public key.
- $K_{I_\mathfrak{N}} = g^{(S_{I_\mathfrak{N}}.S_\mathfrak{N})}$, which needs to be kept secret by Alice. However Alice can verify that it indeed is key based on her shared secret decrypting it using the public key $P_\mathfrak{N}$.

The social networking site stores the pair $\{K_{I_\mathfrak{N}}, I_\mathfrak{N}\}$ in a lookup table. This is useful to perform a reverse look-up of the user identity from $K_{I_\mathfrak{N}}$.

4.2 Stamp Generation Phase

Now, if the user Alice wishes to attach a social stamp to a statement uniquely identified as $\{\mathfrak{T}_i, \mathfrak{W}\}$ on an external site, then the following steps are perfomed:

1. Create the hash $h_i = Hash(\mathfrak{T}_i, \mathfrak{W})$.
2. Generate a large random number r_i, keep it secret.
3. Create the *Binding stamp*: $B_i = K_{I_\mathfrak{N}}.g^{(r_i.h_i)}$
4. Create the *Helper stamp*: $H_i = (K_\mathfrak{N})^{r_i}$
5. Assign the tuple $\{\mathfrak{N}, B_i, H_i\}$ as the anonymous social stamp to the statement $\mathfrak{T}_i, \mathfrak{W}$.

Note that the stamp is bound to the statement only in such a way as to prevent copying the stamp on to a different statement. It however does not prevent anyone else to copy the statement and create their own stamp for it. This should however not affect the security requirements since our intention is to verify if a statement can be linked to Alice, irrelevant of the fact if she had copied that statement from someone else.

4.3 Stamp Verification Phase

When a new customer Bob would like to verify the stamp $\{\mathfrak{N}, B_i, H_i\}$ attached to the statement $\{\mathfrak{T}_i, \mathfrak{W}\}$ then he should be an existing member of the social networking site $\mathfrak{N}$. Assuming he too is a member at $\mathfrak{N}$ with the identity $V_\mathfrak{N}$, he can perform the following steps to verify the stamp and get the social distance:

1. Create the hash $h_i = Hash(\mathfrak{T}_i, \mathfrak{W})$.
2. Transform the helper stamp so that the verifier Bob can be sure that the stamp is indeed bound to h_i by performing the following operation:
$$\bar{H_i} = H_i^h = g^{(P_\mathfrak{N}.r.h)}$$
3. Now contact the social networking site $\mathfrak{N}$ with the tuple $\{V_\mathfrak{N}, B_i, \bar{H_i}\}$ to verify the binding and get the social distance.

On receiving the tuple $\{V_\mathfrak{N}, B_i, \bar{H_i}\}$ the social networking site performs the following operation

1. Use the RSA secret key pair of $S_\mathfrak{N}$ to generate a *de-binder* from the new helper stamp as follows:
$$\begin{aligned}\bar{B_i} &= \bar{H}_i^{S_\mathfrak{N}} \\ &= (K_{I_\mathfrak{N}}.g^{(r_i.h_i)})^{S_\mathfrak{N}} \\ &= (g^{P_\mathfrak{N}.r_i.h_i})^{S_\mathfrak{N}} \\ &= (g^{P_\mathfrak{N}.S_\mathfrak{N}})^{(r_i.h_i)} \\ &= g^{(r_i.h_i)}\end{aligned}$$
The result is due to the property of the RSA keys as shown in Equation 1.
2. Use the de-binder $\bar{B_i}$ to remove the statement related hashed values from the binding stamp by performing:
$$\begin{aligned}B_i/\bar{B_i} &= (K_{I_\mathfrak{N}}.g^{(r_i.h_i)})/g^{(r_i.h_i)} \\ &= K_{I_\mathfrak{N}}\end{aligned}$$
This operation also verifies that indeed the binding was for the statement h_i it was intended for, otherwise the generated key will not be right.
3. The social network can now perform a reverse user identity lookup for $K_{I_\mathfrak{N}}$ in its lookup table to map to the identity $I_\mathfrak{N}$ of Alice as the creator of the stamp. The social network neither knows what the statement was about or where it was posted.

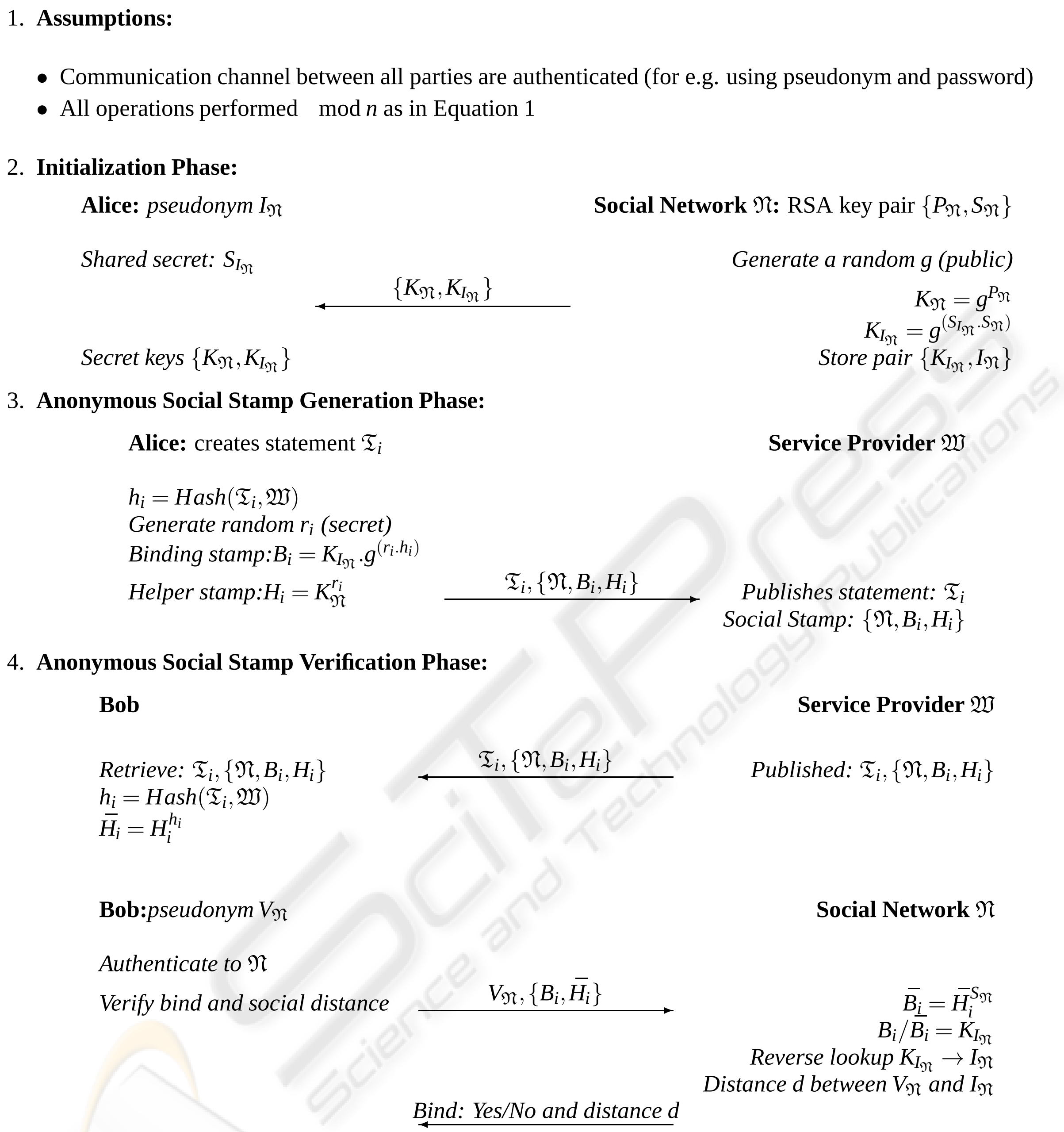
1. **Assumptions:**
- Communication channel between all parties are authenticated (for e.g. using pseudonym and password)
- All operations performed $\mod n$ as in Equation 1
2. **Initialization Phase:**
Alice: *pseudonym* $I_{\mathfrak{N}}$
Social Network $\mathfrak{N}$**:** RSA key pair $\{P_{\mathfrak{N}}, S_{\mathfrak{N}}\}$
Shared secret: $S_{I_{\mathfrak{N}}}$
Generate a random g (public)
$\{K_{\mathfrak{N}}, K_{I_{\mathfrak{N}}}\}$
$K_{\mathfrak{N}} = g^{P_{\mathfrak{N}}}$
$K_{I_{\mathfrak{N}}} = g^{(S_{I_{\mathfrak{N}}}.S_{\mathfrak{N}})}$
Secret keys $\{K_{\mathfrak{N}}, K_{I_{\mathfrak{N}}}\}$
Store pair $\{K_{I_{\mathfrak{N}}}, I_{\mathfrak{N}}\}$
3. **Anonymous Social Stamp Generation Phase:**
Alice: creates statement $\mathfrak{T}_i$
Service Provider $\mathfrak{W}$
$h_i = Hash(\mathfrak{T}_i, \mathfrak{W})$
Generate random r_i *(secret)*
Binding stamp:$B_i = K_{I_{\mathfrak{N}}}.g^{(r_i.h_i)}$
Helper stamp:$H_i = K_{\mathfrak{N}}^{r_i}$
$\mathfrak{T}_i, \{\mathfrak{N}, B_i, H_i\}$
Publishes statement: $\mathfrak{T}_i$
Social Stamp: $\{\mathfrak{N}, B_i, H_i\}$
4. **Anonymous Social Stamp Verification Phase:**
Bob
Service Provider $\mathfrak{W}$
Retrieve: $\mathfrak{T}_i, \{\mathfrak{N}, B_i, H_i\}$
$\mathfrak{T}_i, \{\mathfrak{N}, B_i, H_i\}$
Published: $\mathfrak{T}_i, \{\mathfrak{N}, B_i, H_i\}$
$h_i = Hash(\mathfrak{T}_i, \mathfrak{W})$
$\bar{H}_i = H_i^{h_i}$
Bob:*pseudonym* $V_{\mathfrak{N}}$
Social Network $\mathfrak{N}$
Authenticate to $\mathfrak{N}$
Verify bind and social distance
$V_{\mathfrak{N}}, \{B_i, \bar{H}_i\}$
$\bar{B}_i = \bar{H}_i^{S_{\mathfrak{N}}}$
$B_i/\bar{B}_i = K_{I_{\mathfrak{N}}}$
Reverse lookup $K_{I_{\mathfrak{N}}} \rightarrow I_{\mathfrak{N}}$
Distance d between $V_{\mathfrak{N}}$ *and* $I_{\mathfrak{N}}$
Bind: Yes/No and distance d

Figure 2: Anonymous social stamp interactions.

4. The social network can now inform the verifier Bob (after he has properly authenticated to the social network), the social distance between $I_{\mathfrak{N}}$ and $V_{\mathfrak{N}}$.

This social distance allows Bob to assign a certain amount of trust to the statement rather than assuming it to be a complete stranger. Alice does not have to worry about revealing her interactions at other sites to the social networking site or to be linked across the different sites based on her stamp. Thus all the security and privacy requirements laid down before can be met using anonymous social stamps and still provide the functionality that is required.

More advanced features can be built around this main idea in which the social network allows users to classify users to be more trustworthy only if they are connected through a branch of a particular friend, etc.

5 ADDITIONAL APPLICATIONS

Here we present an extension of the above social stamp concept where the main aim had been to authenticate that a statement had originated from a person in the social network. However, the technique can also be used if the user wants to hide information which can only be read by people within a social distance. Thus additional information can be revealed if the person viewing the statement is within a certain social distance.

To enable the hiding of information, the statement $\mathfrak{T}_i$ needs to be encrypted with the key $Key = K_{I_{\mathfrak{N}}}^{(r_i.h_i)}$. Then the same steps for generation of the stamp is followed as before for the pair $\{\mathfrak{T}_i, \mathfrak{W}\}$.

During verification of the stamp, the social networking site performs all the steps as before to identify the user as $I_{\mathfrak{N}}$. Once the user is identified, the social network knows the shared secret $S_{I_{\mathfrak{N}}}$ and therefore can also re-create the key by performing the following operation:

$$\begin{aligned} Key &= \bar{B}_i^{(S_{I_{\mathfrak{N}}}.S_{\mathfrak{N}})} \\ &= (g^{r_i.h_i})^{(S_{I_{\mathfrak{N}}}.S_{\mathfrak{N}})} \\ &= (g^{S_{I_{\mathfrak{N}}}.S_{\mathfrak{N}}})^{(r_i.h_i)} \\ &= K_{I_{\mathfrak{N}}}^{(r_i.h_i)} \end{aligned}$$

The user $I_{\mathfrak{N}}$ can configure the minimal social distance that needs to be satisfied for the social networking site to release this Key. If $V_{\mathfrak{N}}$ is within this social distance then he receives the Key from social network and decrypt the message $\mathfrak{T}_i$.

6 CONCLUSIONS

We presented the concept of an *anonymous social stamp* which can be assigned to anonymous statements and help prove that the statement was made by a particular member of an external social networking site. Trust can then be derived based on the social distance between the persons concerned: the person who made the statement and the person verifying the statement. A possible implementation of the concept is shown with the existing infrastructure of RSA keys already in use by social networking sites.

This should enable a serious health and well-ness service provider to show testimonials, advices and configurations which can be verified by new customers to belong to people that they would consider trustworthy based on their social distance within a particular social network of their choice. Customers can use any social network of their choice and trust. Service providers would be able to use the trust that people have created by the social networks without having to create a social network of their own.

Additionally we extend the concept to hide information that can be decrypted only by people within a social distance.

REFERENCES

EC (2010a). European healthcare fraud & corruption network (ehfcn). http://www.ehfcn.org/fraud-corruption/fraud-and-corruption-in-healthcare/.

EC (2010b). The unfair commercial practices directive directive 2005/29/ec. http://ec.europa.eu/consumers/rights.

Epinions (2010). http://www.epinions.com.

FTC (2010a). Federal trade commission: Health claims. http://www.ftc.gov/bcp/menus/consumer/health.shtm.

FTC (2010b). Who cares? sources of information about healthcare products and services. http://www.ftc.gov/bcp/edu/microsites/whocares/index.shtml.

Josang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decis. Support Syst.*, 43(2):618–644.

Resnick, P., Kuwabara, K., Zeckhauser, R., and Friedman, E. (2000). Reputation systems. *Commun. ACM*, 43(12):45–48.

Rivest, R. L., Shamir, A., and Adelman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126.