

# Intentions and Intelligent Screening in an Agent-based Personal Communication System

Johan Montelius\* Sverker Janson Jan Gabrielsson  
Swedish Institute of Computer Science Uppsala University

Anders Danne Göran Båge Mikael Eriksson  
Ericsson Radio Systems

## Abstract

We describe a scheme for *intelligent screening* in the context of an agent-based personal communication system.

Intelligent screening is only possible if the called party has knowledge of who the caller is and, more important, knowledge of the callers intentions. We propose an agent-based solution that allows the caller to present both identity and intentions. The scheme uses a metaphor of *business cards* to make the calling and screening procedures easy to understand.

## 1 Introduction

The problem of screening and forwarding incoming calls is mainly a problem of lack of knowledge. In an ordinary signaling system (e.g., SS7), next to nothing is known about the callers identity and intentions. A call center system today would have to rely on the caller's telephone number for the identity, and would have to ask questions ("if you want to speak to an operator please press 0") for figuring out the intentions of the caller. All computer support is on the called party's side and very little support is provided to the caller.

We are exploring an agent-based personal communication system with a view to future computer telephony integrated systems. A network of *personal assistant agents* communicating over the Internet complements voice connections, which are routed through ordinary telephone lines by a switch controlled by the agents.

In this extended abstract, we outline a mechanism for screening of telephone calls, and other forms of communication, based on the metaphor of *business cards*. In the next few sections, we describe the rôle of the personal assistant, introduce the notion of business cards, describe mechanisms of screening based on cards and the management of cards, and discuss security and integrity aspects. Finally we discuss other possible approaches to the screening problem.

## 2 The Personal Assistant

With each user is associated an agent, a *personal assistant* (PA). The PA may be regarded as a secretary who mediates all personal communication, phone calls,

---

\*Contact: Johan Montelius, SICS, Box 1263, S-164 28, Kista, Sweden, jm@sics.se

faxes, emails, etc., and hence has access to all communication media, in particular the telephone network and Internet-like networks.

The user can communicate with the PA through any medium, such as a voice controlled interface over the phone, or through a graphical interface on a workstation.

Like the traditional secretary, the PA will handle both incoming and outgoing calls. For incoming calls, the PA does screening, searching, logging, etc. For outgoing calls, it can help find contact points for the person to be contacted, and, more importantly in this context, provide another PA with information both on the identity of the caller and why the connection is requested. This information will help the other PA in the screening process.

The identity of the caller is easy to provide, but how are intentions expressed? The scheme must provide the screening function with relevant information but also be intuitive and easy to use for the caller. The idea of having a PA to help with communication is not new [2][4] but we think that our approach for handling intentions is new.

### 3 Business cards

We propose using the metaphor of *business cards* to present the intentions of a caller.

A card contains a user identifier (e.g., an e-mail address), a key, and a description. Different cards can have the same user identifier but different keys and descriptions.

For example, Paul might have two cards given to him by his colleague Molly. One  $\{\text{molly@foo.com, key-23, "Molly"}\}$  and another  $\{\text{molly@foo.com, key-65, "Mrs Jones, Foo inc."}\}$ . If Paul wishes to make a private call to Molly he would use his "Molly" card but if he wants to make a business call he would use the "Mrs Jones, Foo inc" card.

When a card is used to set up a call, the PA of the calling part sends a *request* to the PA of the called party. The request will contain the user identifier of the caller and the key of the card used.

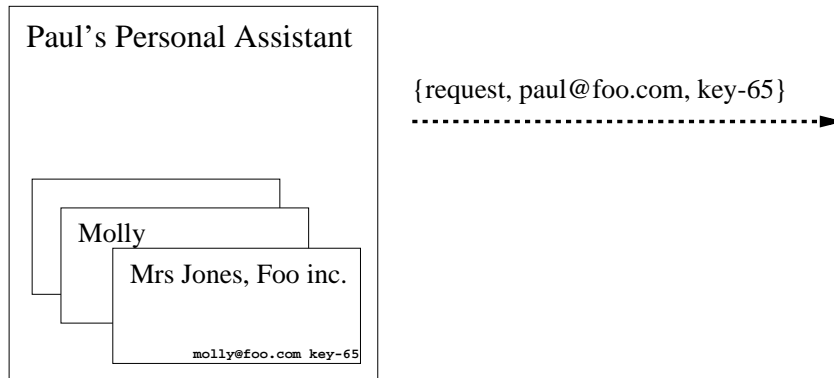


Figure 1: Using a card in a call request

If Paul makes a phone call to Molly, Paul's assistant would send a request containing the user identifier of Paul (`paul@foo.com`) together with either the key `k-23` or `k-65` depending on which card he is using. Figure 1 shows the situation where

Paul has used his “Mrs Jones” card to contact Molly. It is then up to Molly’s PA to decide what to do. It knows that it is a call request from Paul but more importantly it knows Paul’s intentions.

How cards are created and distributed is tightly coupled with the way calls are screened. The sole purpose of having the keys are after all to aid the screening of calls.

## Screening

There are several parameters that decide how screening should be done. Obviously it is important to have a screening procedure that takes into account the time of the day or day of the week, if the user is currently at a meeting etc., but it is equally important to know the identity and intentions of the caller. The least interesting aspect is probably which phone the caller is using and still this is the only information provided today.

The call request will contain the identity of the caller and a key. The key provided in the call request gives information of the callers intentions. Additional information could be obtained, e.g., from the users (digital) calendar and by parameters given by the user. We will not go into details how the screening process could work but concentrate on the use of the key.

We will assume that the identity provided in the request is correct. The “correctness” of the key not as critical. The scheme is mainly a scheme that allows a caller to act politely rather than a scheme that prevents any unauthorized calls to be set up. The scheme will even have emergency keys that will let any call get through. We will talk more about security in the next section.

## Creating a card

A new key is generated for each card that is given away. The description might be the same for many cards but the keys are different. The keys need only be unique to the creator, not worldwide.

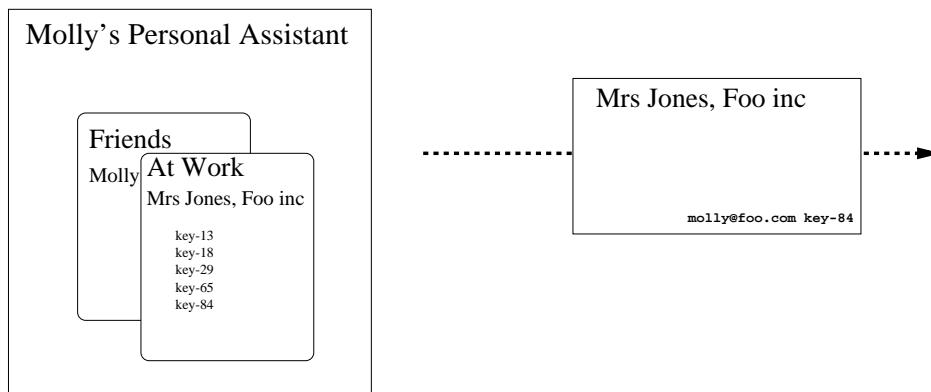


Figure 2: Offering a card also creates a unique key

For example, Molly might have distributed a “Mrs Jones, Foo Inc.” card to all employees at Foo Inc., but all of these cards have a unique key. For easy screening the keys can be grouped, e.g, in a set that could be referred to as the “At work” set.

Figure 2 shows a situation where Molly is offering a new business card to another PA.

Under normal circumstances, the keys would not have to be visible to the user. Cards will be created with a known group as a target and a unique key will automatically be added to the group. A user will only see the name of the group and a template card description for example "At work" and "Mrs Jones, Foo inc".

### Removing a key

By grouping the keys in sets the screening is simplified. For example, if Paul quits his work at Foo Inc., Molly could remove the particular key that was given to Paul from the "At work" set. The screener would then no longer treat calls from Paul with the key `key-65` as an business call.

If nothing is said about a key the screener will treat it as an unknown call. Instead of deleting the key, Molly could move the key to another group called "old colleagues", which has limited access to her during office hours. Paul would then still be able to use his card with the the key `key-65`.

### Offering an alternative

If the PA decides that a call should not be let through it can offer the caller the alternative to leave a voice mail etc. It is, however, also possible to return a business card of a colleague or friend that the the caller could try to contact instead. By providing the caller with explicit alternatives, it is up to the caller to decide whether the the alternatives should be tried. This has been used in the "Open Distributed Office" [3] and seems to be a nice way to avoid the feature interaction problem that may occur when forwarding is automatic.

The business card scheme make it easy to give the right capabilities when alternatives are returned. Paul might (if he's still at Foo inc.) want to give Molly as an alternative when he's called by some one that is using one of his "Paul, Foo Inc." cards. He then gives the "Mrs Jones, Foo Inc." card to the caller but he would never dream of giving away his "Molly" card. This is done automatically by Paul's PA, no interaction with Paul is needed (who is on vacation anyway).

### A database of keys

If the PA keeps track of when a new key was created and to whom it was given. The information could help the PA to do even better screening. A call request could be screened using the knowledge that the key provided by the caller was originally given in a card to someone else.

Maybe Molly wants to treat a call using a key grouped in the "Friends" set differently if it is coming from someone who has not received it in the first place. Friends might not be a transitive relation. Any caller that can provide a key listed in the "Friends" set should however be given a higher priority than a caller that can not show a key at all.

If it is known to whom the key was originally given the to that person can either be punished or given credit to. Paul might be punished for distributing his "Molly" card but Molly could be given credit every time a customer calls the order-reception using a card that was originally given to Molly.

Keeping the time when a key was created could help both in the automatic screening and in the manual management of keys. Keys that were created a long time ago could be removed or moved to a group with lower priorities. Keys that were generated during a certain time period might be removed all together etc.

The possibilities are many but the important thing is that keys are unique when they are created and that the keys them self never give an automatic capability. The received capabilities are decided by the owner of the called PA.

## 4 Security and Integrity

The ability to give away cards is a powerful way of giving access rights to callers, but could also be misused. If Paul deliberately or by accident gives his personal “Molly” card away to a malicious person who posts it on `alt.terror.phone`, strange persons will start to call Molly—not imposing to be Paul but using a key that Molly has grouped in a set called “Friends”. The good thing is that the key is unique, it was given to Paul only and not to all of her friends. The key can therefore be removed from the “Friends” set. Paul can then be given a new card (if he is trusted again) but none of Molly’s other friends have to be notified.

Another scenario is when Molly decides to give higher priority to calls related to a particular project. If she has offered her “Molly, Foo Inc.” card to John, a person at Bar Ltd., she can raise the priority of the corresponding key by moving it to another group and automatically give higher priority not only to calls from John but also from those that John has shared the card with.

Molly could later lower the priority of the key given to John without telling John. He still thinks that he is using a high priority card were in fact Molly has moved on to work with Zot & Sons. This freedom is possible since the key itself does not give any priorities. It is only a mean to put a unique label on the call request.

A card is not unforgeable, but if they are generated with a random number generator they could at least be hard to guess. There is however practical reasons for not having a water tight system that will block all calls that do not have the right key. One example is if Molly’s house is on fire. If the system would prevent her neighbor from calling her at three o’clock in the morning this could have serious consequences.

The scheme needs some sort of publicly known key that anyone could use in an emergency. The social protocol (wake me up again and I’ll call the police) will have to take care of misuse. We don’t think this will be a problem since things would not be worse than they are today.

The usage of keys are related to how capabilities are managed in an operating system. Although security and integrity are important properties of the scheme it should not be viewed as a tool to block unwanted incoming calls, rather a system that allows a caller to behave politely.

## 5 Other approaches

One could use a scheme with fixed publicly agreed keywords, say for example: `urgent`, `business`, `private` and `public`. Such scheme would lack, regardless of how many keywords that are used, the flexibility of the proposed card scheme. To

give higher priorities to a particular group one would have to ask them to use a high priority keyword in call requests. To ask some one to use a higher priority might be flattering but how could one tell someone to stop using for example the `business` key and instead use a `could-wait` key?

Another approach would be to try to describe the intentions of the call. This could be done with for example a list of freely selected keywords. Such list would be very flexible, a business partner could for example use the keyword list ( `my-company`, `project-alpha`, `contract`, `urgent`) to declare his intentions but it would make the screening of calls more complicated. One would have to make an agreement with partners, colleagues and friends to use a limited set of keywords to do the right screening so the scheme would soon be similar to the scheme with a fixed number of keywords.

One could declare the intentions in natural language for example “I would like to talk to Mrs Jones about the alpha contract sometime this afternoon” and leave to the PAs to figure out if and when a call should be set up. This approach, advanced as it might look, is still nothing more than a variation of the keyword scheme.

The problem with any scheme were the caller describes his intentions without the use of unique keys is that the freedom of the screener is limited. In the card scheme that we propose the screener has the control of how to prioritize the calls.

## 6 An Experimental System

We are currently implementing a system to experiment with different approaches. The system is implemented using Erlang [1] a language for telecom applications developed by Ericsson. In its final version it will be distributed over several sites using the Internet for communication between PA's.

The interface for communication between a user and the PA of the user will in the first phase be implemented using graphical terminals. We will later on try to move as much control as possible to a voice interface so that the PA can be controlled using a regular phone.

## References

- [1] URL <http://www.ericsson.se/erlang/>.
- [2] Icchiro Iida, Takashi Nishigaya, and Koso Murakami. Duet: An agent-based personal communication network. *IEEE Communication*, 33(11), November 1995.
- [3] Mike Rizzo, Peter F. Linington, and Ian A. Utting. Call management in the open distributed office. November 1994.
- [4] Mike Rizzo and Ian A. Utting. An agent-based model for the provision of advanced telecommunication services. In *Proceedings of TINA '95*, pages 205 – 218, 1995.