eNumino & aNomino, the IMSI based PKI and protocols to secure the left side of the @[1]

Jean-Luc Schellens

Avenue Edmond Parmentier, 109
1150 BRUXELLES – Belgique
http://www.enumino.org
jlschellens@enumino.org

Abstract: Fighting the annoyance of spam and the dangers of "phishing" is today the top concerns of e-mail service providers (ESP). To simplify the e-mail certificates management; we propose a simple but reliable layer of e-mail authentication, security and confidentiality based on two new and related protocols.

Called “eNumino”, the first one is a way to authenticate an e-mail sender and to deliver him a public key certificate related to his International Mobile Subscriber Identity (IMSI, the E.212 recommendations of the ITU), converted in an Internet Domain Name (DNS). The second called “aNomino” is a way to send double encrypted e-mails via the ESPs without visibility of the sender and recipient identities.

Involving both the ESPs and the mobile networks, these protocols offer a simple but reliable infrastructure for the e-mail’s sender authentication process that can be fully automated and for the e-mail’s exchanges that can be totally anonymized.

Keywords: authentication, anonymity, confidentiality, digital certificate, domain name system (DNS), e-mail, e-mail service provider (ESP), identity based encryption, international mobile subscriber identity (IMSI), phishing, public key infrastructure (PKI), mobile network, security, simple object access protocol (SOAP), spam, spoofing, WS-Addressing, extensible mark-up language (XML).

---

[1] In an e-mail address, the @ symbol is used to separate the identity of the e-mail sender and the domain name of the e-mail service provider.

1 Introduction

Fighting the annoyance of spam and the dangers of fraud activity such as "phishing" is among the top concerns of Internet users and e-mail service providers. "Spoofing," or sending e-mail purporting to be from someone it's not, is an increasingly common and relatively simple way for spammers to pose a security risk when used to deliver e-mail viruses or phisher scams, which attempt to trick users into divulging personal information such as credit card numbers or account passwords by pretending to be from a legitimate source, such as a user's bank.

The rapid developments of these attacks are basically due to the basic weaknesses of the Simple Mail Transport Protocol (SMTP), which in fact sends only postcards[2] and does not require any sort of e-mail sender's authentication.

To fight the spams, different tools are developed to filter the e-mails based on black lists of well-known spammers or on the analyses of the subject lines or even the contents. They are more and more efficient but never completely and are rapidly bypassed by the spammers who mostly react by sending more spams...

A more significant initiative is the Sender ID jointly submitted by Microsoft and Meng Wong to the Internet Engineering Task Force (IETF[3]) standards body. Sender ID aims to prevent spoofing by confirming what domain a message came from and thereby increase the effectiveness of spam filters. But requiring a large adoption by the e-mail service providers, this proposal will in fact only secure the right side of the @!

The use of digital certificate and PKI services is another way to authenticate e-mail sender and to enable legitimate senders to more clearly distinguish themselves from spammers. But until now it requires a relative complex and expensive process for the basic e-mail users - which are rarely ready to visit a notary to certify their e-mail addresses - and it is also poorly implemented by the e-mail service providers which basically are not involved in the certification process.

That is why we propose a simple but reliable authentication and certification process based on two new and related protocols completely involving the e-mail service providers in the fight to secure the e-mail sender's real identity.

2 eNumino

2.1 Definition

Like ENUM[4] (the protocol defined by the IETF), "eNumino" is a protocol to convert an international mobile phone number (MSISDN) first in the corresponding International Mobile Subscriber Identity (IMSI, defined by the E.212[5] recommendations of the ITU and stored on

---

[2] Confusing the users, the e-mail clients display envelopes to symbolize the e-mails…

[3] http://www.ietf.org/html.charters/marid-charter.html

[4] http://www.ietf.org/html.charters/enum-charter.html

[5] http://www.itu.int/ITU-T/worksem/ip-telecoms/e164/e212.doc

the SIM card's "6F07" file) and then in an Internet Domain Name System[6] (DNS) to link it only with secure and anonymous e-mail services.

For instance, the GSM number (MSISDN) "+32 475 12 34 56":

1. Is first converted in the equivalent IMSI: "206.01.475123456" where
   - "206" is the Mobile Country Code (MCC) for Belgium,
   - "01" is the Mobile Network Code (MNC) for Belgacom Mobile and
   - "475123456" is the Mobile Subscriber Identification Number (MSIN);
2. And then in a Domain Name: "6.5.4.3.2.1.5.7.4.01.206.e212.enumino.org".

Unlike ENUM and for security, privacy and users education reasons, the eNumino domain name is deliberately limited to the support of anonymous and secure e-mail services.

Using the IMSI to authenticate an e-mail sender offers key advantages:

- Today, there are far more mobile subscribers than Internet users.
- Compared to the Internet, the Mobile world offers a stronger security and services driven business model.
- The IMSI is an international identification plan for mobile users enabling roaming and billing capabilities.
- A mobile number - unlike an e-mail address - is today really a personally identifiable information (PII), generally authenticated by the mobile network during the activation process.
- By definition, the MSISDN and IMSI are all over the world unique but due to the mobile number portability, the IMSI is more difficult to know even for the mobile subscriber or to guess for outsiders/eavesdroppers.
- The mobile networks are involved in the eNumino registration process (cf. 2.3), in the DN servers' management (cf. 2.2) and up to the e-mail provider's commercial policy, in the deductions of the eNumino registration and services if the mobile subscribers are liable of the payments.
- Messages (SMS and even calls) are exchanged with the mobile user during the eNumino registration process (cf. 2.4) and if necessary during the exchange of public keys between contacts (cf. 5.2).

2.2 The eNumino DNS Hierarchical Naming and Architecture

The eNumino DNS tree structure is based on the three elements of the IMSI and the domain name information are stored in a distributed database contained on DNS name servers, ideally one for each mobile network, storing their portions in DNS zone files and if necessary transferring the subscriber's resource records to the servers of the corresponding e-mail service providers.

---

[6] In a nutshell, the Domain Name System is a service designed to operate on TCP/IP-based networks like the Internet. It implements a hierarchical naming strategy to associate a logical DNS hostname to a corresponding IP address. DNS also supports the delegation of management required in such a large implementation as the Internet.

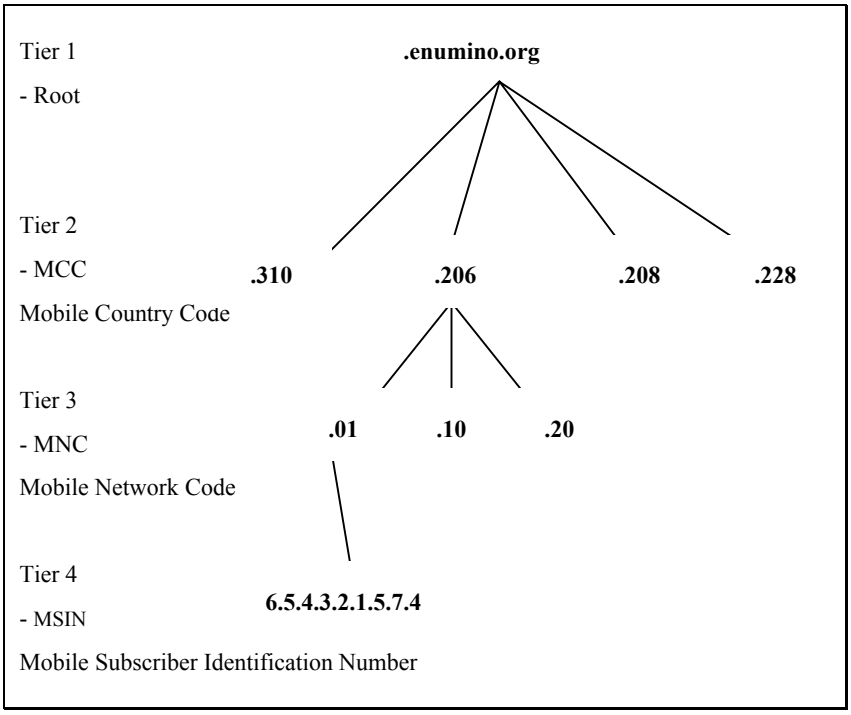

Fig. 1. The eNumino DNS hierarchical naming

In Belgium (206) for instance, there are three mobile networks, respectively Belgacom Mobile (01), Mobistar (10) and BASE (20)[7].

The mobile networks manage the DN servers of the tier 3 with delegation of management and zone transfer to the e-mail service providers being ISPs like Tiscali, Wanadoo or Skynet, or company's e-mail servers of their respective mobile subscribers.

The DN servers of the tier 3 are connected with the Home Location Register[8] (HLR) and the Authentication Center[9] (AuC) of the mobile networks for the eNumino registration process, the permanent update of the DN servers and up to the e-mail provider's commercial policy, the payments by the mobile subscriber of the eNumino registration and the aNomino e-mails.

---

[7] The complete E.212 numbering plans is available at http://www.numberingplans.com/index.php?goto=plans&by=E.212

[8] Inside the Mobile-service Switching Centre (MSC) of each mobile network, the HLR is a database and service control function responsible for the management of each subscriber's records.

[9] Inside the MSC, the AuC is a database concerned with regulation of access to the mobile network.

2.3 The eNumino-Accredited Registrars

Only an e-mail service provider (ESP) is able to become an eNumino-accredited registrar and the accreditation process will imply steps like the ICANN one[10].

Being an accredited registrar, each ESP is authorized to access the eNumino Domain Name system and servers to register new eNumino user and to query existing ones (cf. 4.2).

Each registrar is also able to access the eNumino extranet to exchange a public key with other eNumino-accredited e-mail registrars (cf. 5.1).

2.4 The eNumino Registration Process

As just mentioned, only the e-mail service providers are able to register eNumino Domain Names.

Assuming that Alice is a Skynet e-mail user, the registration process includes the following steps (illustrated in the figure of the next page):

1. With her e-mail username and password, Alice first accesses a secure web page at https://www.skynet.be/enumino_registration.
2. She registers by giving her MSISDN (+32 476 12 34 56), her mobile network and optionally her name and first name.
3. The Skynet's server converts the MSISDN in the corresponding IMSI and eNumino domain name and access the eNumino DNS to check the status of the eNumino:
    a. If the eNumino does not exist in the DNS, the server goes to the next step,
    b. If the eNumino is suspended, the Skynet's server asks first to Alice if she wants to register again before going to the next step;
    c. If the eNumino is active or under registration, the server informs Alice and ends the registration process,
4. If the eNumino does not exist or is suspended, the Skynet's server records in the DN server managing the corresponding MNC:
    - The MSISDN (+32 476 12 34 56)
    - The eNumino of Alice (6.5.4.3.2.1.6.7.4.01.206.e212.enumino.org)
    - The status of the registration: "started".
5. The Skynet's server calls automatically the voice mail of +32 476 12 34 56 to check if it's an active number and sends a SMS asking Alice to confirm her registration.
6. Alice responds by SMS to confirm her registration.
7. Following the confirmation, the server updates in the DN the status of the registration to "confirmed".
8. The ESP's server requests the mobile network to confirm that the MSISDN is active and to know the type of subscription (regular or pre-paid). Following the commercial policy of the ESP, the server deducts also the registration fee from the

[10] http://www.icann.org/registrars/accreditation-process.htm

mobile network. If the ESP offers for free the eNumino registration to its customers, the server bypasses the next step and goes directly to step 10.

9. When the mobile network confirms the payment of the registration fee, the Skynet's server updates the registration status to "paid".
10. The server sends to +32 475 12 34 56 a SMS with an activation code.
11. Alice goes back to https://www.skynet.be/enumino_registration to introduce the activation code and receive a public key certificate issued to his MSISDN and the eNumino public key of Skynet (to be used for the aNomino e-mails defined in 4.1).
12. After the activation, the Skynet's server updates in the DN the status to "active" and adds the IP addresses of its e-mail server(s) in the MX record. For security and privacy reasons, only the following data are registered in the Domain Name of Alice:
    - Her MSISDN (+32 476 12 34 56),
    - Her eNumino (6.5.4.3.2.1.6.7.4.01.206.e212.enumino.org),
    - The status of the registration: "active" which can be updated to "suspended" following the status of the MSIDN in the HLR/AuC of the mobile network (cf. 2.2),
    - The IP addresses of the Skynet's e-mail servers in the mail exchange resource records.

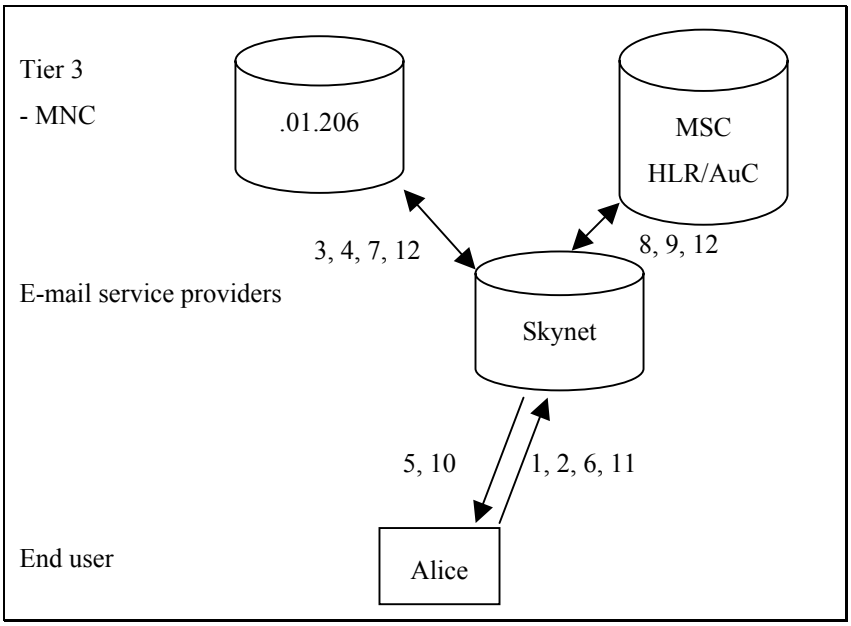

Fig. 2. The eNumino registration and certification process

At the end of the registration process, Alice can certify her e-mails with a digital certificate related to her MSISDN. And the recipients are able to authenticate the real sender of the e-mails and if necessary to call Alice or send her a SMS. In case of spasm or phishing, the recipients are able to take legal action with a reliable authentication of the sender.

An eNumino based e-mail client (cf. 6) is able to organize the incoming e-mails based on the eNumino certificates and the related MSISDNs due to a match in the Alice's address book.

3 The eNumino Based Encryption

We assume that the eNumino certificates can be based on existing public key encryption schemes but being all but an expert in this field, we nevertheless deeply agree with the motivation of Adi Shamir when in 1984 [1] he asked for an identity based encryption in which the public key can be an arbitrary string.

We also want to simplify the certificate management in the e-mail systems. And the IMSI being by definition unique all over the world but far more secured than an e-mail address[11], we would like to have some cryptography experts joining the eNumino concept and protocol to propose a fully functional IMSI-based encryption scheme for the generation of the eNumino certificates where the IMSI would be the arbitrary string, probably with some other system parameters only known by the public key generator.

The IMSI-based scheme could also for instance use the fact that the permanent links between the ESPs and the HLR/AuC of the mobile networks will help in the definition of the expiration date and the revocation of the certificates, knowing that a clear difference can be made between the real mobile subscribers and the pre-paid ones.

The scheme could also take in consideration the fact that more and more PC users have USB memory keys to store and transport their sensible and private data (instead of using a smart cards which are lacking in installed based readers).

4 aNomino

4.1 Definition

The eNumino protocol offers a first layer of e-mail sender's certification, which can highly reduce the number of spams.

To add a higher level of security and confidentiality by simply hiding the e-mail address of the sender and to definitely secure the left side of the @, the aNomino e-mail is a way to send anonymous e-mail by pushing the SMTP protocol to breaking point: only the recipient's e-mail address is valid and is an e-mail address of an ESP, the body of the e-mail being encrypted with the real addressing information – the sender and recipient's eNuminos – and the real content inside!

The aNomino protocol is in fact a mean to put a message in two envelops like in the real life where people first drops an envelope in a post box or at a post office from where the envelope is confidentially brought to the recipient. It uses the public key of the e-mail service provider to encrypt the body of the e-mail (the first envelope) and the public key of the recipient to

[11] Based on the D. Boneh and M. Franklin identity based encryption scheme [2], Voltage uses the e-mail address to encrypt the e-mails or files. See http://www.voltage.com.

encrypt the real content of the e-mail (the second one). That is why we define an aNomino e-mail as a double encrypted one.

4.2 The aNomino E-Mail

Let's assume that Alice is a Skynet e-mail user and that Bob is a Pandora one.

To work correctly and completely, an aNomino e-mail (double encrypted) requires that:

- The Mail Transfer Agents (MTA) are adapted to manage such double encrypted e-mails and the process defined hereafter;
- Pandora and Skynet have exchange - through the process for the e-mail servers (cf. 5.1) - their public keys to allow exchanges of aNomino e-mails;
- Alice and Bob have an eNumino based e-mail client and have exchange their public keys via the Challenge/Response process described below (cf. 5.2).

Then, if Alice want to send to Bob an aNomino e-mail, her e-mail client will create the following SMTP e-mail:

- In the RFC 822 SMTP Header:
  - `From: anomino@skynet.be`
  - `To: careof@skynet.be`
- The RFC 822 SMTP Body of the e-mail being encrypted with the Skynet's public key Alice received at the end of the eNumino registration process.
- The encrypted RFC 822 Body being structured with SOAP/WS-Addressing XML elements (with WS-Addressing[12] - being submitted to W3C by Microsoft, IBM, Sun, BEA et consorts... - you can also define a <messageID>, a <referto>, a <date> element...) to contain the real identifiers (the eNuminos of the sender and recipient) in the <from> and <to> elements,
- The SOAP body element containing the real content of the message being encrypted with Bob's public key.

The outsiders/eavesdroppers just see an encrypted SMTP e-mail send to "careof@skynet.be", any e-mail to "anomino@skynet.be" being automatically rejected by the Skynet's MTA.

The Skynet e-mail server decrypts the e-mail of Alice and in the SMTP body parses the WS-Addressing <from> and <to> elements to find the sender and recipient eNuminos. It checks Alice's eNumino in the eNumino DNS directory to see if the MSISDN of Alice is always active (the mobile is maybe stolen) and checks Bob's eNumino in the eNumino directory to see if Bob is also active and to query Bob's e-mail server being Pandora.

The Skynet e-mail server forwards Alice's aNomino e-mail to Pandora using the same protocol that is a SMTP e-mail with in the From: "anomino@pandora.be" and in the To: "careof@pandora.be", the SMTP body of the message being encrypted with the Pandora's public key. In the SOAP/WS-Addressing, the e-mail server just added its eNumino in the <route> element in order that the encrypted e-mail to Skynet and the corresponding encrypted e-mail to Pandora will be different in length.

---

[12] See: http://www-106.ibm.com/developerworks/library/specification/ws-add/

Again the outsiders/eavesdroppers just see an encrypted e-mail with only a real e-mail address - "careof@pandora.be" - of the e-mail service provider.

When Pandora receives the e-mail, it decrypts it to find the real eNumino of the recipient - Bob - and to deliver the e-mail in his mailbox.

When Bob receive it, his e-mail client checks in the address book if Alice is a whitelisted eNumino user and uses his private key to decrypt the message.

5 The Exchange of Keys through aNomino E-Mails

To work correctly, the aNomino e-mail requires protocols for the exchange of public keys between the e-mail service providers and the eNumino users.

5.1 Exchange between ESPs

Being by definition eNumino-accredited registrars, the e-mail service providers have a secure access to the eNumino extranet to request and exchange the public keys of other e-mail providers. Before the download, the process will include an exchange of signed aNomino e-mails with the responsible contact persons to get her consent about each exchange between e-mail providers.

5.2 Exchange between E-Mail Users

If Alice wants to exchange aNomino (double encrypted) e-mails with Bob, she sends an aNomino e-mail where the real content:

- Is inevitably not yet encrypted with Bob's public key but signed with Alice's private key
- Is structured in a XPIML (eXtensible Privacy and Identity Markup Language, a XML schema currently under development) based document to manage:
  - Up to 3 Challenges/Responses about respective personally identifiable information (PII) Alice and Bob know about each other (e.g. date of birth, last college, number of children, date of last face to face, first name of spouse, brother or best friend…)
  - An agreement about the use of the exchanged public keys ("no forward" for instance)
  - With the Alice's public key as attachment.

The Alice's e-mail provider checks the eNuminos (cf. 4.2) and the signature of Alice, holds a copy of the XPIML document, leaves blank the responses and forwards the e-mail to Bob's e-mail provider.

After receipt, Bob answers the responses - if necessary by sending Alice a SMS or even calling her to check - and sends a aNomino e-mail back via his e-mail provider to the Alice's e-mail provider with his public key and signature.

The Alice's e-mail provider checks the responses of Bob with the original XPIML document. If the responses of Bob match the Alice's ones, the Alice's e-mail provider sends the key of Bob to Alice and the Alice's one to Bob (again via an aNomino e-mail to the Bob's e-mail service provider).

Alice is now and for good able to send double encrypted aNomino e-mails to Bob and vice versa. And they are respectively "white listed" in their address books.

6 An eNumino Based Application

To illustrate the eNumino & aNomino concepts and protocols, we are developing a plug-in for Outlook, the most popular e-mail client for Windows, or Thunderbird 0.7, the Mozilla's next generation open source e-mail client. The following screen captures show the main menus of the solution we call "Netmino"! Such an application could be freely distributed by the ESPs to promote the eNumino & aNomino deployments.

In the first menu, the user can register at eNumino via the e-mail provider and activate the services after the delivery of the activation code.

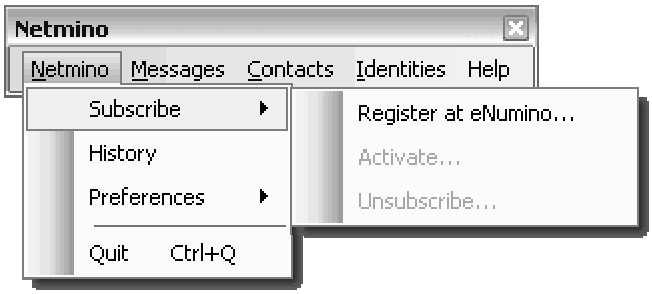

Fig. 3. The menus to register at eNumino via the ESP

In the next one, the user can send certified e-mails or double encrypted aNomino e-mails to the contacts.

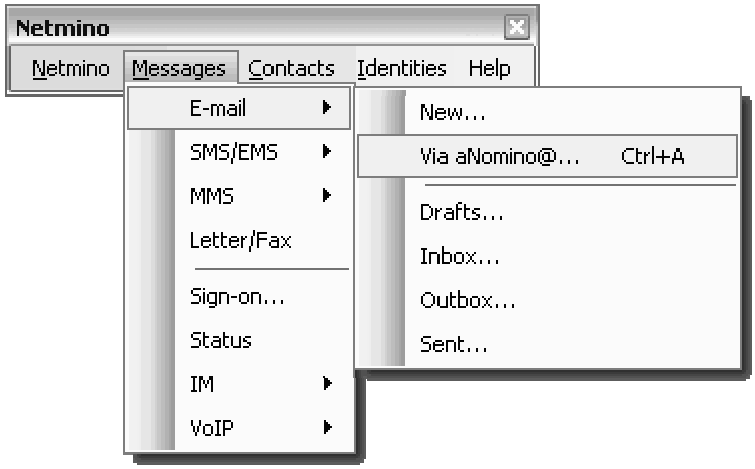

Fig.4. The menus to send eNumino certified e-mails or aNomino e-mails.

Hereafter, the user can query the eNumino directory – but not the eNumino DNS reserved to the e-mail service providers – to retrieve other eNumino users based on their mobile numbers (MSISDN).

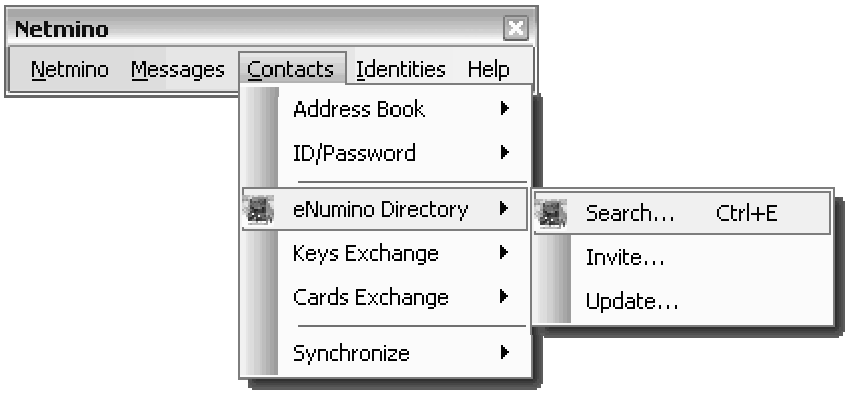

Fig. 5. The menus to search other eNumino users.

An application like Netmino would also be able to automatically organize the incoming e-mails in different folders following the level of security:

1. One for the aNomino e-mails;
2. One for the eNumino certified e-mails;
3. Another for the e-mails coming from the not certified contacts in the address book (with an automatic response inviting them to register at eNumino);
4. A “quarantine” for all the others.

7 New Levels of E-Mail Privacy, Confidentiality and Security

The eNumino & aNomino concepts and protocols offer key advantages to fight against the annoyance of spam and the dangers of fraud activity such as "phishing":

- To authenticate the real e-mail sender - and not only the right side of the e-mail address – the eNumino protocol uses the IMSI, an all over the world unique personally identifiable information (PII) which is due to the mobile numbers portability, more and more difficult to know for the mobile subscriber or to guess for an outsider.
- The IMSI is just stored in the eNumino DN servers for the links with the mobile networks but converted in the corresponding MSISDN to contact the mobile subscriber during the public key certification process, when a recipient receives an eNumino certified e-mail or to take legal action in case of spam or phishing.
- The e-mail service providers are the only eNumino-accredited registrars with the collaboration of the mobile networks.
- Only the ESPs have an access to the eNumino DN servers.

- The management of the certificates is also jointly dependent on the ESPs and the mobile networks.
- The expiration date of a certificate is based on the type of mobile subscription (regular vs. pre-paid) and the certificate is automatically revoked when the subscription is stopped for any reason.
- The eNumino protocol offers a first layer of e-mail sender's certification relatively easy to deploy by the ESPs.
- The aNomino e-mails offer a higher layer of security and confidentiality by sending double encrypted e-mails where the real identities of the sender and the recipient are invisible for the outsiders/eavesdroppers.
- The aNomino e-mails can also be used for a simple but secure exchange of public keys and for the update of revoked ones
- The aNomino e-mails can also serve for the exchange and automatic update of personal information like credentials.

8 Conclusion

The fight against spams requires a combination of national and international legislations, technical developments and user education and action. The eNumino & aNomino protocols are new steps in this direction, combining both technical developments and user involvement.

These protocols are based on the existing public key encryption schemes even if the Adi Shamir's request for an identity based encryption can promote the developments of new schemes based on the IMSI, an all over the world unique personally identifiable information (PII).

Involving both the e-mail service providers and the mobile networks, these protocols offer a simple but reliable infrastructure for the e-mail's sender authentication and certification process that can be fully automated and for the e-mail's exchanges that can be totally anonymized.

References:

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", in Advances in *Cryptology - Crypto '84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47-53, 1984.

[2] D. Boneh and M. Franklin "Identity-Based Encryption from the Weil pairing", in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003. Extended abstract in proceedings of Crypto '2001, Lecture Notes in Computer Science, Vol. 2139,Springer-Verlag, pp. 213-229, 2001.