telnic
The .tel registry

Protecting .tel Contact Data

ABSTRACT

The .tel top-level domain (TLD) is a new domain created exclusively for publication and sharing of contact information in real time. The contact data is published directly in the DNS in the form of NAPTR (naming authority pointer) resource records, which include the type of contact (email, home phone, IM, etc.), the contact itself, its priority and label as entered by the domain owner. To ensure protection of personal information, the .tel platform includes a privacy model defining encryption and decryption of such information. Mechanisms implementing the privacy model for .tel data are described in this paper.

Table of Contents

REFERENCES

1. RFC3403, http://tools.ietf.org/html/rfc3403
2. "NAPTR Records in .tel", September 2008, http://dev.telnic.org/naptr.pdf
3. IETF http://tools.ietf.org/html/draft-timms-encrypt-naptr-01
4. RFC3761, http://tools.ietf.org/html/rfc3761
5. IANA Enum services http://www.iana.org/assignments/enum-services
6. ENUM Implementation Issues and Experiences, http://ietfreport.isoc.org/idref/draft-ietf-enum-experiences/

CONTROLLING ACCESS TO DNS RECORDS

With your own .tel, you have complete control over how people contact you. And you probably would not want all the people on Earth to know your mobile phone number, although you'd share it with your friends and family. To enable this kind of discretion, a privacy mechanism is needed. As the DNS is universal and provides answers to anyone, a novel approach was required.

The .tel solution provides a multi-level privacy protection system using well-tested methods:

- **Communications protocol protection**: access is via secure HTTPS connection
- **Secure data publication**: DNS records encrypted with complex algorithms
- **Peer-to-peer data access**: protected contacts encrypted and stored individually for each authorized user
- **Data distribution**: encryption keys and encrypted data maintained by separate organizations in independent secured databases
- **Secure authentication**: access to the keys database protected by credentials known only to the user, including a custom challenge question and answer
- **Password protection**: passwords maintained in a hashed and not plain-text format

COMMUNICATIONS PROTOCOL

HTTPS, the secure HTTP connection over encrypted Secure Sockets Layer (SSL), is used for all security-related operations. This holds true both for the web interface, and for all .tel client applications that support private data handling.

SECURE DATA STORAGE

Within a .tel domain, all contact information is stored in NAPTR resource records [2]. A NAPTR holds a small number of well-defined fields, and only some of them may contain sensitive information that requires protection.

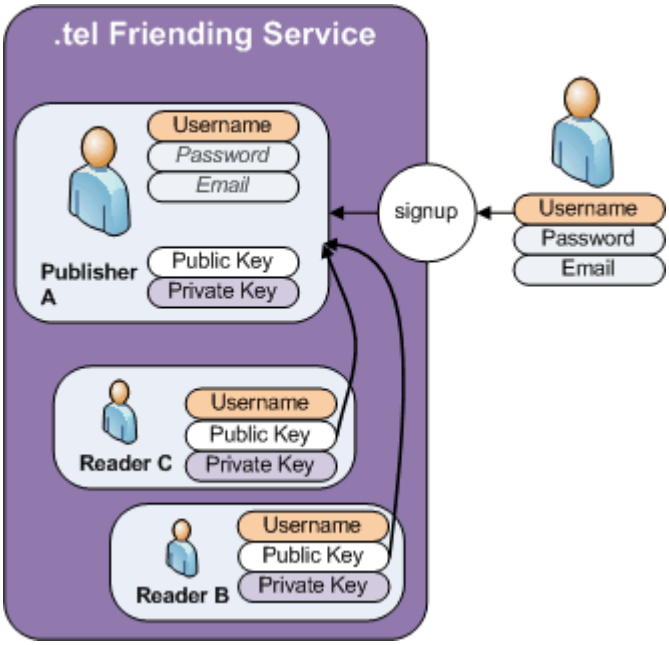
All NAPTRs can be stored and retrieved in a normal way, but the x-crypto Enumservice of a "protected" NAPTR [3] clearly indicates that the record requires special processing. Client applications not interested in encrypted NAPTRs can then discard this record and continue processing others.

To protect NAPTR records, they are encrypted using a complex asymmetric algorithm, 1024-bit RSA with PKCS#1.5 padding. In simpler words, each record is encrypted with a 1024-bit public key created by multiplying two large numbers. The data can then be decrypted by a private key that contains information on those numbers. The public-private key pair is unique for each .tel domain owner, and each authorized user gets the private key to decrypt the protected data.

In a "protected" NAPTR record, all fields are encrypted except the order and preference fields. This allows a user to change those fields (and so that contact’s position in the list) without data re-encryption. For example, when going into a meeting, Alice (who owns alice.tel) may swap the preferred order of contacts, but she's unlikely to enter completely new information. This approach will reduce the processing load on the provisioning system and will enable pre-encryption of plain text fields to speed up construction of protected NAPTRs.

DATA ACCESS MODEL

In the .tel model, a domain owner publishing private data for someone is a **Publisher**, and the person who has the key to read this protected data is a **Reader**. As shown in the figure to the right, each potential Reader has a Public/Private key pair to read encrypted data. The Publisher encrypts private data for each Reader by using the appropriate Public key, and the Reader uses the associated Private key to unlock the data.



Connections between publishers and readers are called "friending" relations, so that .tel domain owners can be "friends" of other .tel domains or users, thus granting them access to sensitive information. Those connections are tracked by the Sponsoring Organization (SO), Telnic Ltd.

Client .tel applications can also implement logging into the SO member system and managing friending relations. In this case, the client application needs to store the username and password for the SO system, as well as friending relations. The application also needs to recognize an existing friend relationship a queried .tel domain and redirect the DNS query to the sub-domain designated for the querying Reader. Because each secure sub-domain contains a copy of both public data and protected contacts for this Reader, the client application needs to make only one DNS query to retrieve all data.

ELECTRONIC HANDSHAKE

To allow someone to read your private data, you need to establish a friending connection with this person, which is done by an *electronic handshake*. At the user level, this means sending a "friend request" message and getting a positive response. At the system level, the electronic handshake includes exchanging messages between the Publisher and the Reader, and subsequent provision by the Publisher of the dedicated subdomain with encrypted NAPTR records. In these messages, the Reader tells the Publisher where to find his/her public key, and the Publisher tells the Reader the sub-domain where private data for that reader will be published. All transactions assume that both the Reader and the Publisher have accounts in the Sponsoring Organization. After a friend relationship has been established, the Reader account gets a backup record showing the relationship in the Publisher Store.

After the successful electronic handshake, the Reader's client program has a local record of the relationship, (or can query for the current list to the Publisher Store) and so queries the sub-domain with private data instead when asked for the publisher's contacts.

DISTRIBUTION OF SENSITIVE INFORMATION

Encrypted DNS records for each .tel domain are published on name servers maintained by appropriate registrar organizations. At the same time, encryption keys are stored separately from the data itself, in the Sponsoring Organisation (SO) systems. This way, even unauthorized access to any system does not grant access to protected contacts.

The SO has a member database independent of the .tel domain owner database; a user in the SO system can be associated with zero, one or multiple domain names. For each user (active and guest), the SO maintains the following data:

- Credentials: Hashed values of ID, API password, challenge question and answer
- Passphrase-protected public-private key pair
- List of friending relations with Publishers
- Queue of friending request and response messages that are used to establish Publisher-Readers relations; see Use Cases below for examples of such messages.

SO User Types

Sponsoring Organisation systems distinguish the following types of users:

Guest users - have not registered a domain but have signed on and so can read private data generated for them.

Full (active) users - have registered .tel domains, can read private data published for them by others, can publish private data for their friends, and can choose to have search directory entries for each of their registered domains.

Declined users - have indicated that they do not want to engage in the features supported by the Sponsoring Organisation.

Vestigial users – have just registered a domain and have a one-time account in the Sponsoring Organization with a temporary username and password.

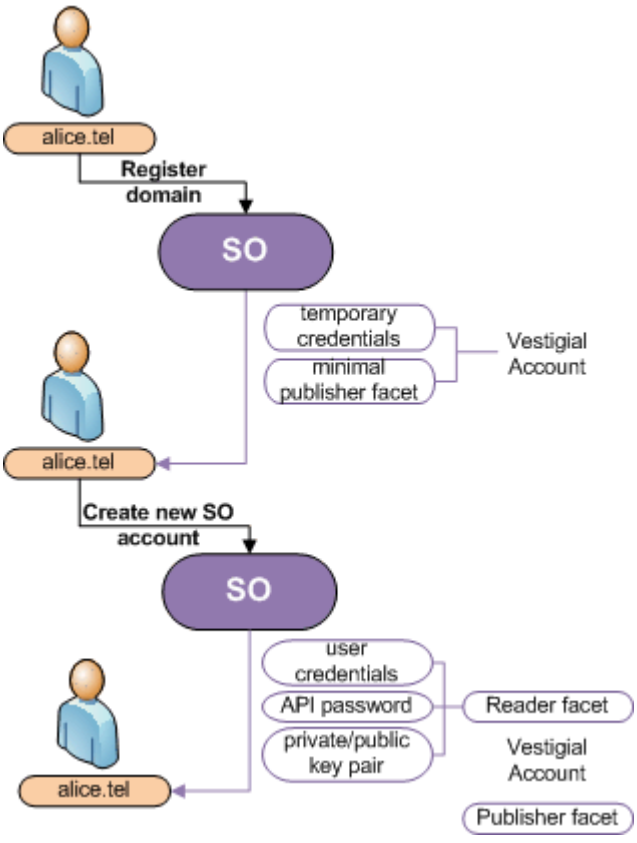
USE CASES

The following use cases illustrate processes related to the .tel privacy model.

Becoming an SO Member

Let's imagine that Alice has registered alice.tel. She will get a username and password for managing her .tel domain from her registrar. She can provision data and publish it in DNS just using this Registrar account. However, to share private data, Alice also needs an SO account. It's Alice's first domain, so the system creates a new SO account for her. Subsequent domains that Alice buys can be associated with the same account.

When Alice registers her domain, the Sponsoring Organisation automatically creates a vestigial account with a "one-time" identity and credentials, and sends an email to Alice with a link to a "sign on" web page it maintains.



When Alice first enters the SO system, she submits a request to create a new SO user account using the temporary credentials supplied in the email. The SO member system allows Alice to select a Username and web password for her new account, and to choose a secondary challenge question and response for those times where confirmation is required. With that, the SO generates a unique ID for this account with an API password and a public/private key pair. As a result, a new full member account is created.

Now Alice is ready to send and receive friending requests.

Friending

Alice wants to make Gary a friend to exchange private contact data. She tells him all about .tel and gives the SO login page address, so that Gary can log in as a guest user (Gary cannot be a full member because he has no .tel domains) and read Alice's private contacts.

In the SO system, Gary creates a friend request message (FRqM) for Alice, which reads like this:

```
From: A1352F.reader.nic.tel
To: alice.tel
Date: Thu Mar 1 16:59:26 GMT 2009
Message-type: Friend Request
Key-domain: a1352f.reader.keys.nic.tel

Cover-note: Hi Alice. It's Gary, we met
down the pub. You told me to join you!
```

The request message is stored in the SO message queue, so that when Alice next logs in using her client program, she will see the pending request. Because Alice likes Gary, she will confirm the relation and send a friend response message (FRsM) back to Gary.

```
From: alice.tel
To: A1352F.reader.nic.tel
Date: Mon Mar 5 15:34:17 GMT 2009
Message-type: Friend Response
Sub-domain-id:
Aabbccddeeff11223344556677889900feeddcc
Cover-note: Yes, Gary, I remember you!
```

After the connection is established, Alice knows where to find Gary's public key, and Gary has added alice.tel to his list of publishers with links pointing to the sub-domain where Alice publishes private information. His client programs will know where to look for private data.

This sub-domain is a 40-char label related both to the sender and the recipient and is unpredictable to anyone other than Alice. If Alice is no longer Gary's friend, she simply stops publishing private contact data at that domain name.

Establishing a friending relation between two full members, like alice.tel and bob.tel, is analogous to the case with the guest user Gary, except Bob (by owning bob.tel) will have a full member account.

Publishing Encrypted NAPTRs

Individual "protected" NAPTR records have the Enumservice type x-crypto, which has been designed not to break IANA ENUM service type formats [5] and abide by the IETF "ENUM Experiences" document [6]. Publication of an individual record is described in this section.

To publish private contact information at alice.tel, Alice's client application looks up each Reader's public key in the DNS, encrypts private data for that Reader with the respective key and publishes encrypted data in designated sub-domain. In this example, Alice has pre-populated her alice.tel domain and has become friends with Bob. She wishes to encrypt two NAPTRs in her domain for Bob's viewing only.

1. Alice obtains Bob's public key from the public key repository, the `reader.keys.nic.tel` zone file, for example:

```
bob.reader.keys.nic.tel. IN KEY

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1o6BKfnC4yqd1lB/uZPR1+DliVnE7V
7EUU8M8YPI4RtsGxlm9TpwPWaMc4OmYmg9/AxbYucr0jVUEjFlAXAsUGpKyEnzvklQAlX
grJmdOL+1pLXdcz1AYOkHKH+/qTc5/1f4Siiau3HVVndojFUG88ukgsKgFaZj6sN+pR9o
ZFQIDAQAB
```

2. Alice takes the binary representation of the NAPTR and encrypts all fields of the record except the order and priority fields as the plain text:
   `"u" "E2U+fax:tel" "!^.*$!tel:+441234567891!"`
3. Alice encrypts the record with Bob's public key and encodes the result with Base64.
4. Alice encrypts all private NAPTRs that Bob is allowed to see in a similar way and publishes them in the defined sub-domain. Bob's client program knows the sub-domain name from the friending response message, and will query this transparently.

SUMMARY

Contact information published in .tel domains is under full control of the domain owner, and can be secured against unauthorized access by encrypting individual records and publishing them in secret sub-domains for each user with appropriate access rights. Complex encryption and authentication mechanisms ensure that the sensitive information is safe. To gain access to private information, a user must be registered with the Sponsoring Organization and must have explicit permission from the domain owner to view that information.

At the same time, the .tel architecture enables client software to implement SO authentication and optimized data retrieval. For examples and guidance on implementing this functionality, please refer to the Developer's Manual, http://dev.telnic.org/docs/devguide.pdf.