Report on the 3rd ENUM Day of 28 September 2004 held in Frankfurt am Main

In the context of the continuing ENUM test operation, the responsible registry, DENIC, organized the third ENUM Meeting on 28 September 2004. Its principal subject was the security of Voice over IP. ENUM is a new technology that bridges the gap between telecommunications and the Internet. Thanks to ENUM and the ENUM services, it is possible for subscribers to use their existing telephone numbers to gain access to the entire world of telecommunications. Some 140 participants with various interests in the subject, including numerous DENIC members already offering ENUM domains, telecommunications service providers and academics, discussed the progress that ENUM had made in Germany in the months before the meeting.

Agenda

1. Welcome and introductory summary
2. Technical background
3. Telephone-number validation
4. Innovation policy
5. Practical experiences in the field trial
6. Further inputs from trial participants

1. Welcome and Introductory Summary

Welcome (Sabine Dolderer, DENIC eG)

The participants were welcomed by Sabine Dolderer, a member of DENIC's Executive Board, and the meeting was conducted by Petra Blank, a member of DENIC's ENUM project team.

Progress made within the ENUM project (Stefan Dieterle, DENIC eG)

According to Stefan Dieterle (DENIC's ENUM project manager), ENUM was picking up speed. Since the second ENUM Meeting in March 2004, the number of providers handling the registration of ENUM domains had more than doubled. Users were already able to choose from amongst 43 providers. An even faster increase, namely 227%, had been recorded in the number of ENUM domains (up from 260 to 850). This was a figure that might appear miniscule compared with the large number of telephone lines. However, it was possible to use just one single ENUM domain to run a whole telephone installation with several hundreds (and even thousands) of extensions, meaning that the number of ENUM users would be very significantly higher than the number of domains. Most of those already using ENUM were developers or others with an in-depth technical interest, who were involved in evaluating the potential of the new technology with a view to being able to offer services and applications at the earliest possible date.
Stefan Dieterle reported that DENIC had been very actively involved during the preceding half year both at ENUM information events organized by others and through its own information events (training seminars for its members). Guidance on where to find the accompanying material was included in the

slide presentation that he used to illustrate his talk: http://www.denic.de/media/pdf/enum/veranstaltungen/Stefan_Dieterle_DENIC_Status_Quo.pdf. This included not only a summary of other project activities that DENIC had indulged in up until then, but also work within the standardization bodies who had been dealing with the ENUM protocol. He also commented on the prospects for the quarter year to follow and announced a number of important forthcoming dates.

2. Technical Background

2.1 SIP security (Prof. Dr. Andreas Steffen, ZHW (Zurich University of Applied Sciences Winterthur))

One of the main focal points of the ENUM Meeting was the issue of how best to tackle security in connection with the use of VoIP, which was tied in with concepts for coping with the problem of spam over Internet telephony (or "SPIT" for short). In both cases, there are crucial roles for authentication (i.e. the question as to whether the purported sender of a message really is the sender) and protection against data espionage and data falsification. The speakers presented various models for possible solution strategies for the future. One speaker was Professor Dr. Andreas Steffen of the Zurich University of Applied Sciences Winterthur (http://www.zhwin.ch), who was working on security issues at the technical-protocol level of the ENUM standard. He advised operators of SIP services to work with authentication mechanisms, such as http Digest Authentication, to make sure that it was not possible for unauthorized persons to make use of their SIP services.
For signalling, on the other hand, there were various procedures available for use. One possible solution for end-to-end security was Secure Mime (S/Mime); however, little research had been done into the use of certificate-based solutions for SIP services in a global environment. It was possible to use TLS (Transport Layer Security) for security in that layer, which worked in a similar manner to making Internet pages secure by means of cryptography (https). The addresses for the use of this protocol would then be called: sips:user@domain. Provisions had already been made for both TLS and S/MIME in the SIP standard (RFC3853); it had, however, not yet been implemented for the vast majority of applications. At the ZHW, there was an ongoing dissertation project to gain experience with this security add-on to SIP.

In the network layer, it is possible to achieve security through the use of IPSec. IPSec is a secure variant of the traditional Internet protocol and can thus be used independently of the SIP applications. The media data is transmitted by means of RTP (RFC and RCTP (RFC3550). Suitable means for providing security are the protocol add-ons Secure RTP–SRTP and Secure RTCP–SRTCP (RFC3711). In the network layer, it is also possible to use IPSec.
Andreas Steffen has made the full version of his article available for general consultation at http://security.zhwin.ch/DFN_SIP.pdf. The slides accompanying the presentation are available at http://www.denic.de/media/pdf/enum/veranstaltungen/ENUM_SIP.pdf.

2.2 Future potential of VoIP technology (Nils Ohlmeier, Snom)

The problem of spam over Internet telephony (SPIT) had been identified and given a name, and possible solutions had been proposed for it, before it even arose and was distributed millions of times over (which was what had happened with e-mail SPAM). Nils Ohlmeier of Snom, http://www.snom.de,

stated that all the developers and users were in complete agreement that the correct time to create effective early protection for VoIP had already arrived. He went on to give an overview of the methods that were suitable for that purpose and that had already been put forward by the IETF with a view to standardization. His presentation analyzed various categories of SPIT and proposed scenarios for counter-measures and is available at:
http://www.denic.de/media/pdf/enum/veranstaltungen/ENUM_Tag_DENIC_04_snom.pdf.

2.3 DE-VoIPX as a privacy solution for the ENUM system in Germany (John-Erik Horn, toplink-plannet)

John-Erik Horn of toplink plannet GmbH (http://www.toplink-plannet.de) presented his idea for a pure Internet-based telephone network for Germany, to which he had given the name "DE-VoIPX". It was a concept that he had initially developed as a university thesis. ENUM would be used throughout the whole country to route calls. It would be a network in which the subscribers (SIP servers) would build up a relationship of mutual trust on the basis of the use of strong authentication mechanisms (certificates). Thanks to this trusting relationship, it would be possible to guarantee the existing requirements as regards secure communication (for instance authentication of the communication partners and the integrity of signalling messages). Such a network would also provide a response to the whole problem of levying charges for use. John-Erik Horn's presentation met with extremely interested reactions from his listeners. For many, it was the first time that they had been confronted, in particular, with the requirements that would be necessary for the Internet infrastructure once VoIP technology came to cover a large proportion of telephony. In dealing with security, John-Erik Horn presented several avenues being explored that might lead to solutions, but his own proposal to set up a network founded on in-built trust (De-VoIPX), although a particularly promising one, would also entail intensive outlay. Detailed illustrations of the various scenarios are to be found in his slide presentation:
http://www.denic.de/media/pdf/enum/veranstaltungen/Horn_DeVoIPX_DENIC_Vortrag.pdf

3. Telephone-Number Validation

3.1 Validation at Portunity (Björn Rücker, Portunity)

An additional procedure for telephone-number validation had become available in July 2004. Many of the field-trial participants were already using it, and final users were also finding it acceptable. Björn Rücker of Portunity (http://www.portunity.net) presented this procedure from the registrant's point of view, but emphasized that it could be used by all registrars. A precise description is to be found at http://www.portunity.net/article17390-3083.html.
Björn Rücker stressed that his view was that the final users had not yet properly grasped the full scope of ENUM's potential and felt that wider dissemination of the existing knowledge ought to be one of the priorities for the immediate future. In order to get this particular message across, he had prepared an impressive ENUM demonstration. Espousing the motto "*eine Nummer für alle Dienste*" ("a single number for all services"), he showed how an incoming call could be put through to various different terminal devices making use of ENUM technology. If it happened that the person called was not accessible at any of them, the system could still put the call through to an e-mail address, which the recipient was free to determine at will.
There was an intensive debate on Portunity's validation procedure with very divergent views. It was recognized that it had a clear advantage in being acceptable to end users and that it facilitated a quasi-instantaneous validation of the telephone connection and the registration of the ENUM domain without

needing to chop and change between media. One disadvantage that was voiced was the fear of abuse, which, of course, also existed for conventional telephone connections, as one of the participants interjected. It was noted that the procedure was in the process of undergoing evaluation as regards its acceptance and practicability within the ENUM trial. Up until then, no consideration had been give to legal aspects.

3.2 Validation with the FUZZY! tool (Eberhard Franke, FUZZY! Informatik)

Another possible form of validation, which could also be used to support other procedures already in use, was presented and explained by Eberhard Franke of FUZZY! Informatik AG (http://www.fazi.de). As a company, FUZZY! sees itself as a solution provider for data quality management, especially as regards processes that are critical for a particular undertaking in relation to information concerning its business partners. The basis for its data records is Deutsche Post's database and its internal directory underlying the published telephone directory. This is then followed by qualification according to streets and/or telephone numbers. A validation – and thus a check of contents, applying logical validity – detects missing or faulty items directly during input or in the data records already stored. After identifying faulty or missing items, FUZZY! proceeds to correct the records.
The system ensures that the records are kept up-to-date. One of its techniques for doing this is to update the postal addresses once or twice every week; another is to keep the telephone numbers up-to-date as per the latest working day by performing 50 000–100 000 updates per day. The proportion of entries that concern mobile telephony does not exceed 8-10% of the total.
In an online demonstration via a web interface, Eberhard Franke showed the capabilities of the software available for checking and correcting incomplete and faulty items of data. A precondition for its use, however, is that the record sought must be in Deutsche Post's database or in the German telephone directory, which means that there are certain number blocks and ranges as well as certain users that are not covered.
Eberhard Franke stressed that he was interested in working together with a trial participant to build up the procedure so that it could be integrated in special organizational routines run by ENUM service providers. In answering a question, he stated that the costs for processing a single query would be, first of all, around EUR 0.15 as a royalty to Deutsche Telekom for using its data material and, secondly, another EUR 0.15 as a payment to FUZZI for the provision of the services and the data interface. The set of slides accompanying this presentation are available at:
http://www.denic.de/media/pdf/enum/veranstaltungen/FUZZY-ENUMI.pdf.

3.3 IP-2-IP accessibility from the German (0)800 service numbers (Michael Volpert, DTMS)

The next presentation was made by Michael Volpert of DTMS, and his subject was "IP-2-IP accessibility from the German (0)800 service numbers", which makes it possible to exploit synergies in adjusting accessibility by means of service numbers based on the German public telephone network (PSTN) as well as those based on ENUM. DTMS is the operator of a PSTN covering the whole of German territory. It is specialized in service numbers based on an intelligent network (IN) of its own and is the country's second biggest provider in the field of service numbers. According to the speaker, it might be possible to create synergies in the following areas:

- uniform routing control for service providers (load balancing)
- uniform routing features / additions to accessibility features that it is difficult to implement in a classical intelligent network
- uniform accessibility and load statistics

- end-to-end protocols through to service providers with a "VoIP island" (accessibility convergence)
- reduction in first-hand costs through the use of existing "non-PSTN" network elements
- accessibility from all networks for service numbers at reduced interconnection costs (especially F&I costs)

It is particularly thanks to the reduction in the interconnection costs that there is potential for new business models. These are savings that can be passed on to final customers, provided they take the incoming call via VoIP. The presentation was accompanied by a set of slides illustrating the scenarios: (http://www.denic.de/media/pdf/enum/veranstaltungen/ENUM_800_Denic_280904.pdf).
Michael Volpert went on to present an overview of the various procedures in use at the time for carrier pre-selection in PSTNs. He pleaded strongly for the yardstick for the validation of ENUM domains not to be made more severe than that applicable for the carrier-pre-selection method.

4. Innovation Policy

4.1 Need to be proactive in regulatory and innovation policy as far as ENUM is concerned? (Dr. Volker Leib, Nexus Institute Berlin)

In presenting the above-mentioned topic, Dr. Volker Leib, a social scientist at the Nexus Institute (www.nexus-institut.de) in Berlin, tackled the subject of ENUM from a non-technical perspective. His view was that the Internet, VoIP and ENUM were major innovations, which would lead to fundamental structural changes, some of which had already taken place. One of these was going to be a radical change in the years to follow in the technical foundation underlying telephony. Large telecommunication undertakings, such as Deutsche Telekom and British Telecom, were already working on the assumption that their conventional telephone networks would be decommissioned within a period of 5-10 years and replaced with IP networks based on Internet technology. Despite that, the current telephone numbers would remain in use, as would the more than two billion telephone connections existing throughout the world. He therefore put in a plea for a forward-looking policy on innovation – one which would provide a framework for the future development, such as to guarantee legal and planning certainty for the undertakings involved. In addition, it would have to be made easy for providers of VoIP services to join the market. He saw it as "tremendously important" in moving forward that "we do all we can to be able to start the regular ENUM operation as soon as possible and to make sure that the transition from the current test operation to the regular operation does not suffer on account of unnecessary complications". He finished by reminding the audience of the attractive grant programmes available to companies involved in developing technology, which had been set up by both the German federal government and the European Union. Further information on these was available at: www.bmbf.de, www.bmwa.bund.de and www.it2006.de. The slides that accompanied his presentation are to be found at:
http://www.denic.de/media/pdf/enum/veranstaltungen/Vortrag_Leib_2004-09-28.pdf.

5. Practical Field-Trial Experience

5.1 Do it yourself: ENUM/ VoIP in 24 hours (Ulrich Keil, AmEuro Ventures GmbH)

During the session on "Practical field-trial experience", Ulrich Keil presented a brief report on the experience that AmEuro Ventures GmbH (http://www.ameuro.de) had had with VoIP. Its first two

attempts to build up a VoIP telephone system with the involvement of established providers had failed. It had then resorted to open-source software and created and implemented a solution of its own. He supported his positive testimonial with numerous hints on how others could emulate his company's successful solution as described in his presentation, the slides of which are available at: (http://www.denic.de/media/pdf/enum/veranstaltungen/AEV_vortrag.pdf). Ulrich Keil then demonstrated a test run of his system, in which it functioned perfectly.

6. Other inputs from trial participants

Edgar Scherer of the UdS (Saarland University) contributed a number of remarks on the practical experience with his project. It had by then grown to be one of the biggest and best-known VoIP projects with ENUM support in Germany and still had spare capacity to take on further users. The UdS offered its students VoIP services, and each one was allocated their own individual telephone number. Detailed information was to be found on the project's own webpages at: http://www.rz.uni-saarland.de/projekte/VoIP/.

In addition to the URLs indicated above, the presentations and supporting documentation are also available at http://www.denic.de/en/enum/allgemeines/veranstaltung/ENUM-Tag.html.