



enum.at
net.communications

ENUM Validation in +43

Otmar Lendl

ENUM.AT

RIPE 50 --- ENUM WG

Content



- Intro
- Flashback to RIPE45
- What didn't work out as planned
- New Requirements
- Solution:
 - Token
 - Trust relationships
 - Usage patterns

Validation



enum.at
net.communications

The person in control of the ENUM domain must at all times be authorized by the owner of the corresponding E.164 number.

- *Initial Validation*
Checking the rights at delegation time
- *Recurring Validation*
Ensuring that any changes in the ownership of the E.164 number are reflected in the ENUM domain space.

The Cast



- RTR-GmbH
 - Regulatory body
- enum.at
 - Tier 1 ENUM Registry
- Registrars
 - Companies who actually sell ENUM domains
- Validation Entities
 - Organizations which check number use rights
- Telcos
 - “Kommunikationsdienstebetreiber” (KDB/CSP)
- End-user

Back at RIPE45



- Validation requirements
 - scalable = fully automatic
 - easy on incumbents
 - **online, synchronous verification of right-to-use**
 - handle number reuse correctly
- Proposed solution
 - telcos know their customers, often electronically
 - export number, password into DB, place a RADIUS server on it
 - have a trusted third party link those servers into a „circle of trust“
 - all validation transactions pass through the TTP, which creates signed Validation Tokens.
 - re-validation is different from initial validation

Problems encountered



- If the incumbent doesn't cooperate this scheme fails.
 - Incumbent refused to cooperate if anything they do can be reused by a competitor.
 - The regulator refused to force them to cooperate.
- If Registrar and Telco are identical this makes things quite complicate as they must use an external party to talk to themselves.
- Good for fully automatic system, was overkill for initial, paper+FAX based schemes.
- The scheme was too complex to get the system off the ground.
 - We needed something to be up and running by 2004/12.

Requirements: TNG



enum.at
net.communications

- Must cope with all possible role settings:
 - Registrar = Telco = VE
 - Fully segregated roles
 - Everything in between
- Auditable
- Non-repudiation of responsibility
- Motto:
 - Make the first baby steps possible
 - Ability to scale to a fully automatic system where multiple actors cooperate

Changes

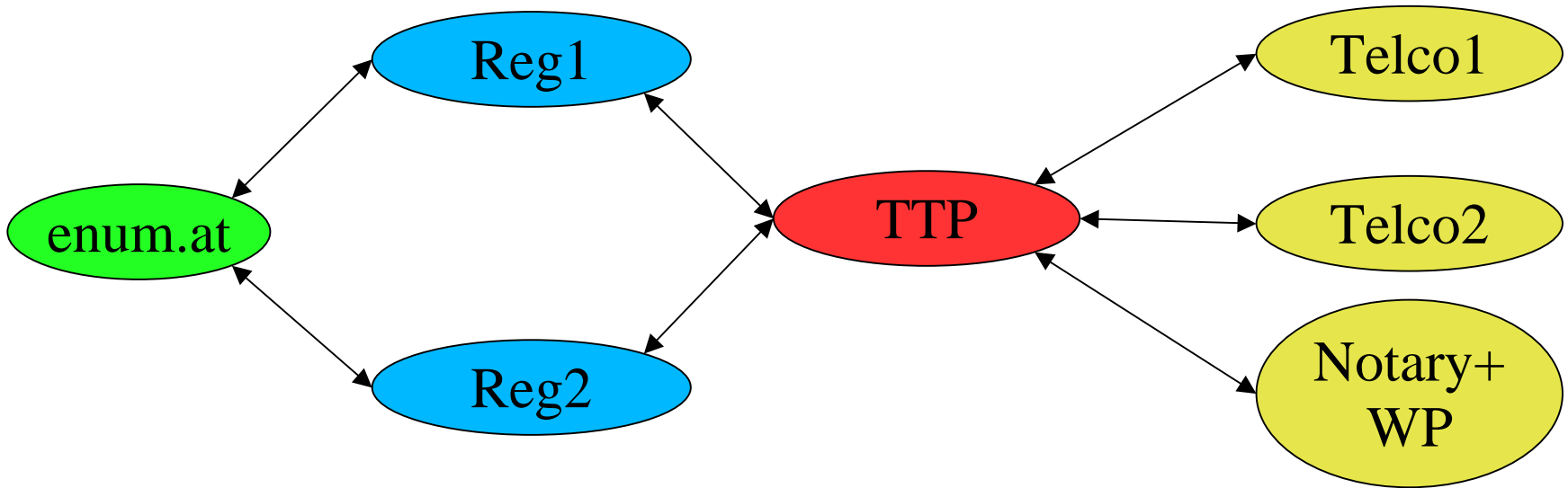
- No single TTP / Validation Entity
- Cooperation between players is not required
 - But if they choose to cooperate, we still get the fully automatic system.
- Any registrar is free to run his own VE.
(Our experience shows that he does.)

Validation Methods

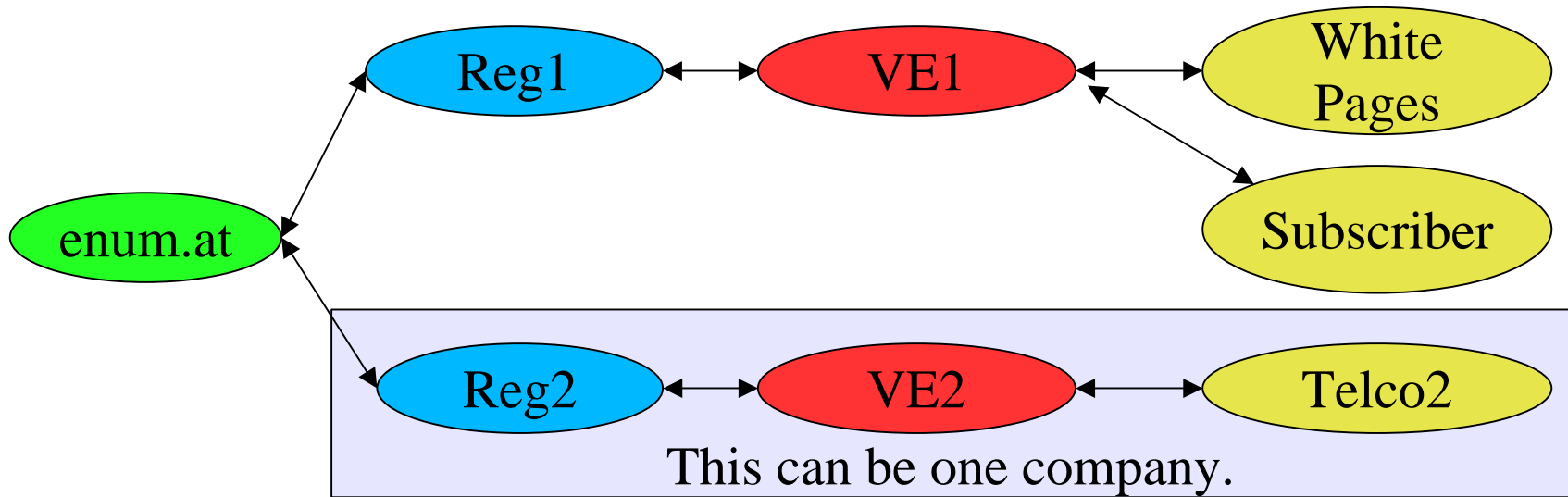


- The setup does not specify how validation is done.
 - nor does it define a protocol between registrars, VEs and telcos.
- It only defines:
 - how validation results are represented
 - a trust model
 - how validation results are communicated to the Tier1 registry
 - How to keep track on what methods were used

Removing the single TTP



Removing the single TTP



The Validation Token



enum.at
net.communications

- The Validation Token is a digitally signed XML-document with which the VE guarantees to the Tier1 that the validation was successful.

Token Content

- Required fields
 - E.164 Number
 - Registrar
 - Validation Entity
 - Validation Method used
 - VE specific serial number
 - Timestamps (valid from/to)
- Optional fields
 - Subscriber Name
 - Address
 - VE-specific data
- XML-SIG signature
 - Enveloped signature with an embedded X.509 cert.
 - No PKI infrastructure is assumed.

Token example



enum.at
net.communications

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="http://www.enum.at/rxsd/enum-token-1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
    "http://www.enum.at/rxsd/enum-token-1.0 enum-token-1.0.xsd">
  <validation serial="XYZ-12345">
    <e164number>+4317654321</e164number>
    <validator>12</validator>
    <registrarid>1101</registrarid>
    <method>42</method>
    <createdate>2005-04-07</createdate>
    <expiredate>2005-10-07</expiredate>
  </validation>
  <tokendata>
    ... name / adress / email / whatever
  </tokendata>
</token>
```

Token Signature

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="http://www.enum.at/rxsd/enum-token-1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation=
    http://www.enum.at/rxsd/enum-token-1.0 enum-token-1.0.xsd
  Id="TOKEN">
  <validation serial="XYZ-12345">
    <e164number>+4317654321</e164number>
    <validator>12</validator>
    <registrarid>1101</registrarid>
    <method>42</method>
    <createdate>2005-04-07</createdate>
    <expiredate>2005-10-07</expiredate>
  </validation>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#TOKEN">
        <Transforms>... </Transforms>
        <DigestMethod ...</DigestValue>
      </Reference>
    </SignedInfo><SignatureValue>...</SignatureValue>
    <KeyInfo><X509Data>...</X509Data></KeyInfo>
  </Signature>
</token>
```

Token Standardization



- XML Schema specified
- Seamless integration into EPP
 - The complete EPP frame including the token must pass an XML schema check.
- ID submitted to the IETF ENUM WG
 - draft-mayrhofer-enum-validation-00.txt
- Implementation as a Perl module is available on www.enum.at

Wider Applicability



- Specialized TLDs with strict rules on eligibility
- Sunrise phases (e.g. .eu)
- Telephone number portability verification
- Data-format for direct number assignment

Usage Patterns



- Up and running:
 - Registrar with in-house VE generate tokens based on number-portability checks.
 - The www.my-enum.at portal:
 - VE for mobile numbers based on SMS loops.
 - External VE (based on RTIR), SOAP interface.
- Future:
 - Telcos may offer token-generation to customers
 - All the fancy cross-domain authentication schemes we dreamed about

We're in production



- This is not just theory.
 - 3.4.e164.arpa is up and running in production service since December 2004.
 - Three independent implementation of the Token generation exist.



enum.at
net.communications

+43 780 ENUM meets the PSTN

Otmar Lendl

ENUM.AT

RIPE50 --- ENUM WG

Content



enum.at
net.communications

- Intro
- Basic principles
- Number assignment
- PSTN Routing
- Porting
- Tariffs

Numbering rules



enum.at
net.communications

- +43 numbering plan is defined by the RTR
- “Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung - KEM-V” ordinance.
 - Current version from 2004/05/12
 - Defines rules for number use (e.g. geographic vs. nomadic use)
 - 0720 for generic use

+43 780 Summary



- The ENUM delegation is a prerequisite for a number assignment.
- New number allocation procedure. Neither block-assignments, nor individual delegation.
- The destination of the call must be on the Internet as indicated by the ENUM record.
- All originating telcos are allowed to bypass the normal PSTN interconnect by terminating directly to the VoIP URI.

Number use



- To get numbers, you need to provide a communication service based on ENUM.
 - The final communication endpoint must be reachable via the Internet
 - You can't just use them as aliases for geographic numbers
 - Routing via ENUM is authoritative
 - It doesn't need to be voice calls

Number Assignment



- Old style
 - Block assignment
 - Individual assignment
 - Once you have a number, you can get the ENUM domain.
- 0780
 - Get the ENUM domain first
 - It's a prerequisite for the official number assignment.
 - Numbers are still assigned to telcos (CSPs), but in non-contiguous blocks.
 - These CSPs have to provide gateways

Call Routing

- In Austria, there is neither
 - an automatic routing between telcos (No counterpart to BGP4)
 - nor a central database containing routing information for all numbers.
- Old Style
 - All telcos have to route calls via SS7 interconnect to the telco owning the block.
 - Number portability is done with Onward Routing (think ICMP Redirects for phone calls)

Initial 0780 Routing



enum.at
net.communications

- Number are only assigned to a CSP which arranged for the existence of a Gateway:
 - This CSP can terminate calls via his own gateway.
 - All other telcos can use the old method of routing calls to owner of the block.

0780 Routing



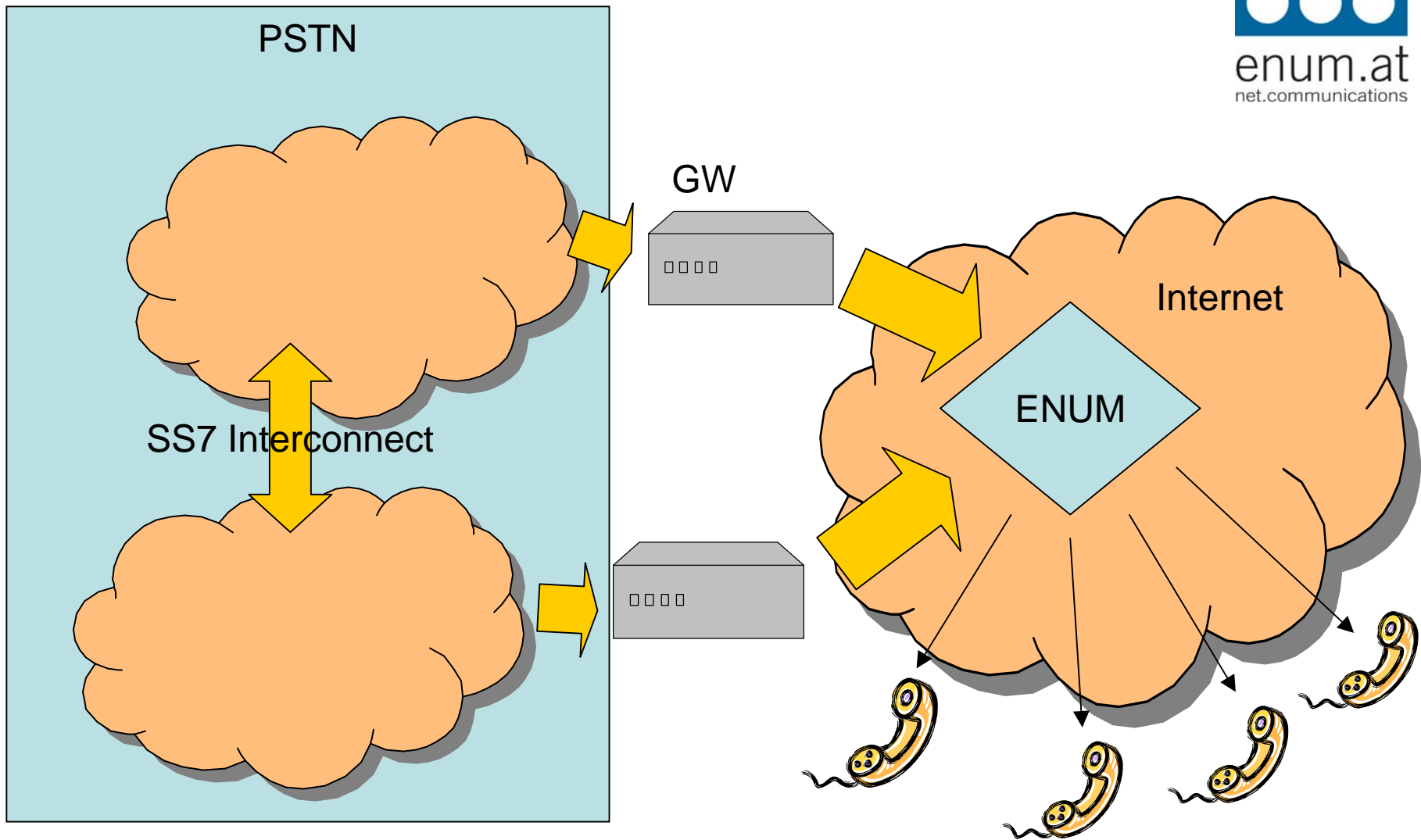
enum.at
net.communications

- Once there are multiple gateways
 - All gateways can terminate calls to all 0780 numbers
 - The originating network chooses the gateway
 - There is no requirement to route to the number-owning telco
 - All networks are free to build their own gateway and terminate all calls locally
 - There is competition amongst the gateways.
- Gateways in the other direction are independent
- Building gateways is easy: see <http://www.enum.at/index.php?id=380> for a how-to with a Cisco 5300.

0780 Routing



enum.at
net.communications



Porting in 0780



enum.at
net.communications

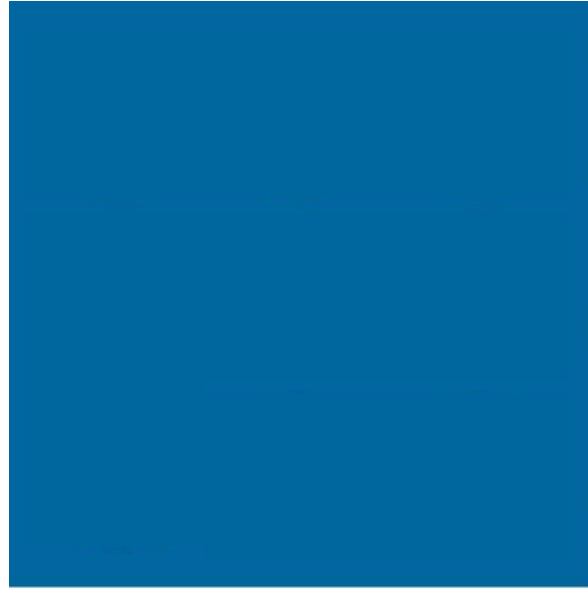
- Number Porting = Change of the CSP-ID within the ENUM-Registry
- No impact on the routing in the PSTN
- No impact on the routing via ENUM
- No impact on the number assignment paperwork

Tariffs



enum.at
net.communications

- Costs are not regulated, the originating network can set them freely.
- Market forces are supposed to keep them reasonable.
- What do we expect?
 - Initial similar to 0720 and corporate numbers (somewhere between local and national calls)
 - Competition between gateways drives down IC-fees
 - Any telco can implement its own gateway → calls to 0780 can be terminated locally.
 - Longterm: tariffs will be similar to network-internal calls.



enum.at
net.communications

phone: +43 1 5056416
office@enum.at
www.enum.at