TELEPHONE NUMBERS IN AN IP ENVIRONMENT

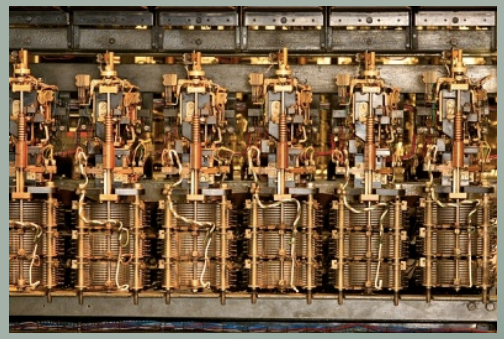
Henning Schulzrinne
FCC & Columbia University
March 26, 2015

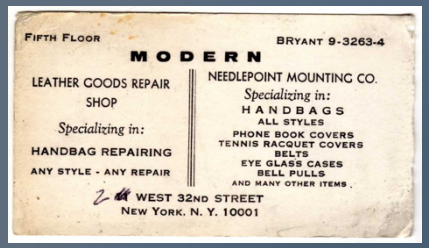
Overview

- Meta-assumptions
- Why phone numbers?
- Architecture options
- Data
- Operations

Disclaimer: Examples tend to be US-specific – mostly because of my lack of familiarity with other numbering domains.

Phone number evolution





Communication identifiers

Property	URL owned	URL provider	E.164 phone numbers	Service-specific
Example	alice@smith.name sip:alice@smith.name	alice@gmail.com sip:alice@ilec.com	+1 202 555 1010	www.facebook.com/alice.example
Protocol-independent	no	no	yes	yes
Multimedia	yes	yes	maybe (VRS)	maybe
Portable	yes	no	somewhat	no
Groups	yes	yes	bridge number	not generally
Trademark issues	yes	unlikely	unlikely	possible
I18N	technically, yes; humanly, no		yes	?
Privacy	Depends on name chosen (pseudonym)	Depends on naming scheme	mostly	Depends on provider "real name" policy

Communication identifiers

- Need identifier that
  - can work on different media
  - can be conveyed orally
    - try spelling email address…
  - can work internationally
  - is portable across organization
  - does not reveal too much
  - provides rough hint of geography & time zone
- →
  - I18N → number
  - portable → no provider domain
  - portable, privacy → no personal name
  - geography → country-level assignment
- Alternative:
  - all app-world
  - cryptographic identifier (public key) in address book

Phone numbers for machines?

< 2010

212 555 1212 →

254 mio.

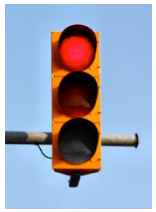
500 123 4567
(and geographic numbers)

OnStar by GM

12% of adults

500 123 4567
533, 544 →

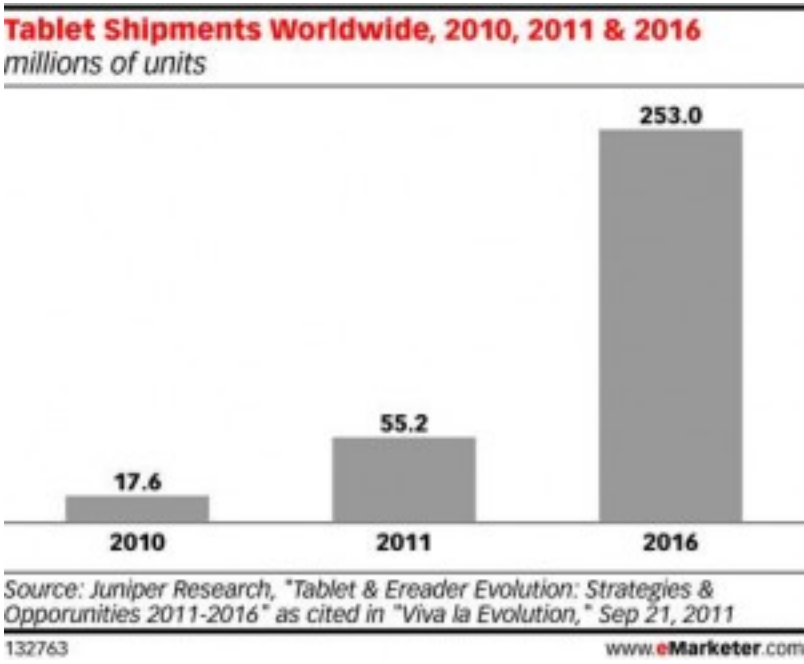
5 mio.



311,000

64 mio.

44.9 mio.



now: one 5XX code a year…
(8M numbers)

10 billion +1 #'s available

Phone numbers are valuable

In fact, cellphones have been proliferating in the city so rapidly that state regulators were notified on Friday that Manhattan will need yet another area code by late 2017.

Neustar, the company that manages the national phone-numbering system, told the Public Service Commission that all of the 646 numbers could be used up by then. Neustar's filing did not divulge what the new area code would be.

Theoretically, there are about 7.9 million phone numbers available per area code. It took about 45 years to use up all of the 212 numbers, but it will take only about 20 to exhaust the inventory of 646 numbers.

Weeks before signing a lease on an apartment on the Upper West Side, Mr. Lippitt, 36, purchased the phone numbers from a broker who buys and sells them. Normally, phone numbers are assigned without cost, but for several years 212 numbers have been selling for anywhere from $75 to more than $1,000.

NY Times, March 25, 2015

Meta-assumptions

- ~~"We've always done it this way"~~
- Old: policy(t_1) ➔ implementation(t_1+T)
- New: technology platform(t) → policy(t_1), policy(t_2), policy(t_3)
- All "regular" numbers, including free-phone ("800#")
  - avoid being too +1 specific
- Possibly others: SMS short codes, CICs
- Scalable, reliable, trustworthy, neutral, …

Out of scope of my discussion

- Short-term changes to numbering administration
- Global “root”, with uniform policies
- Change numbering policies, contracts, …
  - e.g., who can get numbers (but this may change – see FCC iVoIP discussion)
  - differs between number spaces (800 vs. others)
  - doesn’t seem to affect protocol architecture, just scale

Number administration is baroque

NANC

advises

FoN
LNPA
NOWG

NAPM

NPAC Number Portability Administration Center

National Pooling Administration
PAS - Pooling Administration System

atis

Reconsider assumptions?

- NANPA, LNP, LERG, RespOrg, … separation?
  - NANP Administration System (NAS)
  - Pooling Administration System (PAS)
  - Number Portability Administration Center (NPAC)
  - ➔ *Number Administration Database*?
- numerous separate databases with often unclear data flows and opaque business models (e.g., CNAM, BIRRDS, LERG)
- portability is limited in arcane ways (rate center)

Sample policy variables

- Who can get what kind of numbers?
  - carriers and other telecommunication providers
  - organizational end users (companies)
  - individuals
- What rights do number holders have?
  - Can they sell the number?
  - Pass it on to others?
- In what units?
  - 1, 100, 1000?
- Are numbers restricted (in use or portability)?
  - by geography (NPA? LATA? rate center?)
  - by service (mobile, SMS, “freephone”)?
- Who pays for what?
  - manage scarcity by administrative rules or economic incentives
  - one-time or periodic renewal (800#, 10c/month)
- What attributes are associated with a number?
  - Who can read & write those attributes?

Who are the actors?

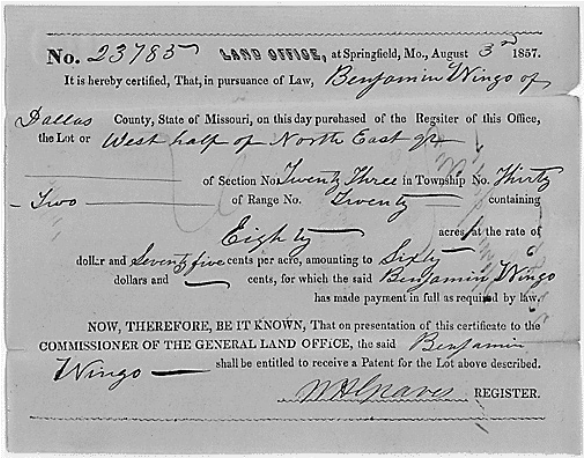
- Service providers: carriers, hosted providers (“cloud”), self-provisioned large enterprises, RespOrgs, …
  - some obtain numbers for their customers
  - some just route to them
- Number management entities
  - registrars, registries
- Third-party verifiers [TPV] (e.g., for porting)
- Property validators (for numbering meta data)
  - Experian, Dun & Bradstreet, Neustar, government agencies, …
- Consumers
- Regulators
- Others?

Additional numbering uses?

- TCPA (“robocalling”)
  - is this number a cell phone or a landline?
- Validated or asserted attributes
  - “extended validation”
  - e.g., geographic location, registered name, licenses

Role of MODERN

- "Title registry"
- → create a clear record of number use and history
- associate attributes with numbers
  - some semi-public, others private



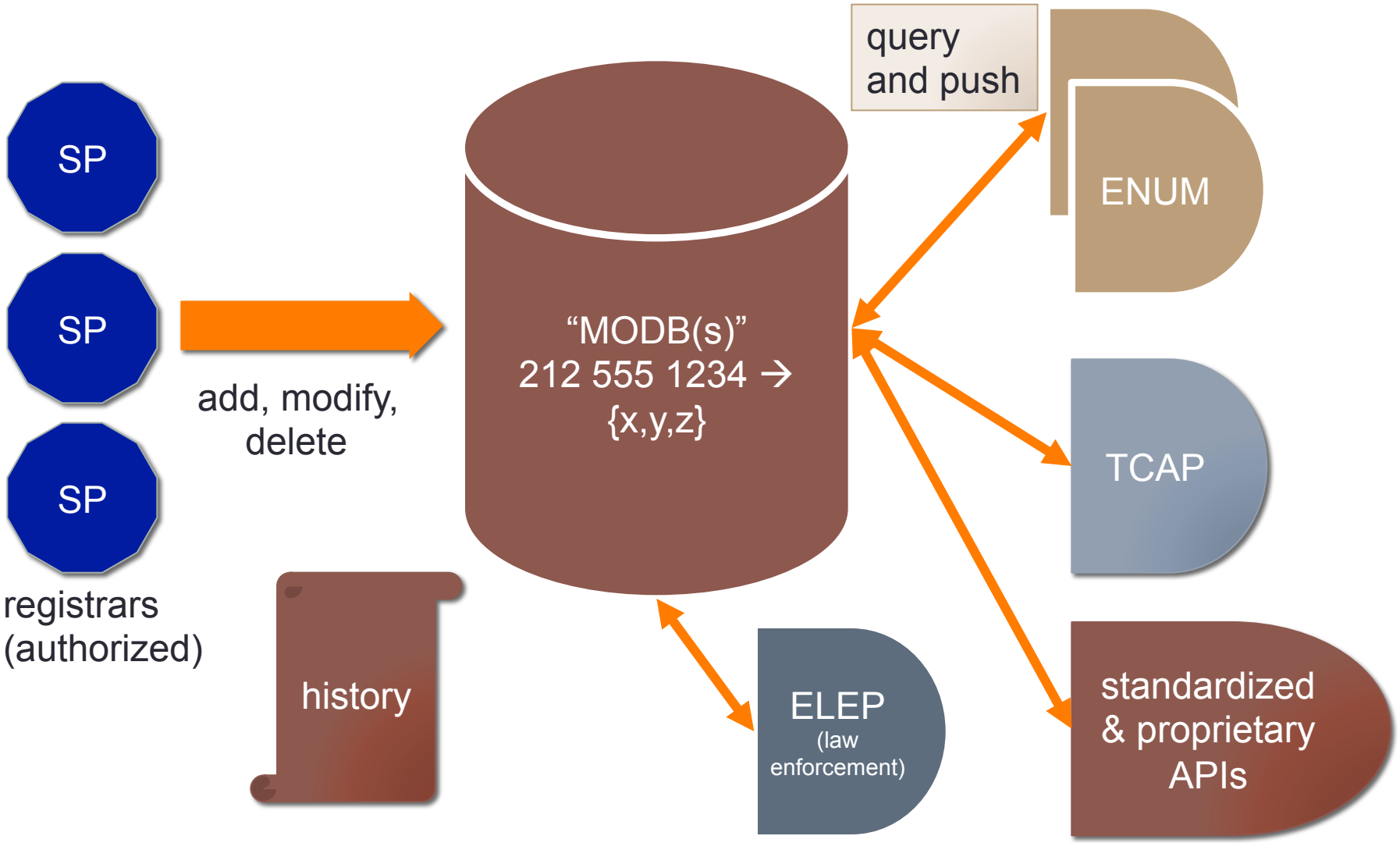
No. 23783 LAND OFFICE, at Springfield, Mo., August 3 1857.

It is hereby certified, That, in pursuance of Law, Benjamin Wingo of Dallas County, State of Missouri, on this day purchased of the Register of this Office, the Lot or West half of North East ¼ of Section No. Twenty Three in Township No. Thirty Two of Range No. Twenty containing Eighty acres at the rate of dollar and Seventy five cents per acre, amounting to Sixty dollars and cents, for which the said Benjamin Wingo has made payment in full as required by law.

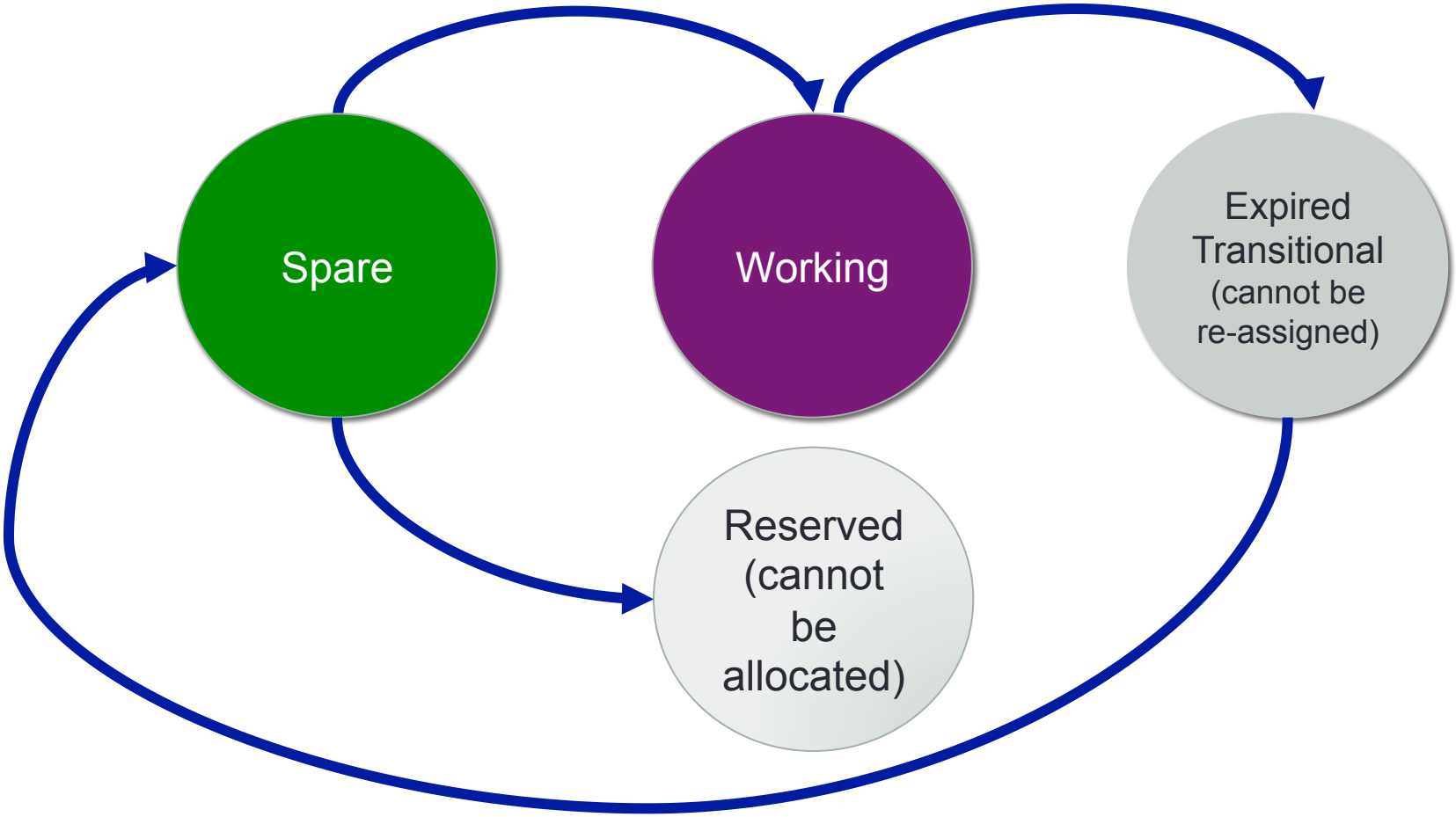
NOW, THEREFORE, BE IT KNOWN, That on presentation of this certificate to the COMMISSIONER OF THE GENERAL LAND OFFICE, the said Benjamin Wingo shall be entitled to receive a Patent for the Lot above described.

W. Pearce REGISTER.

Big picture

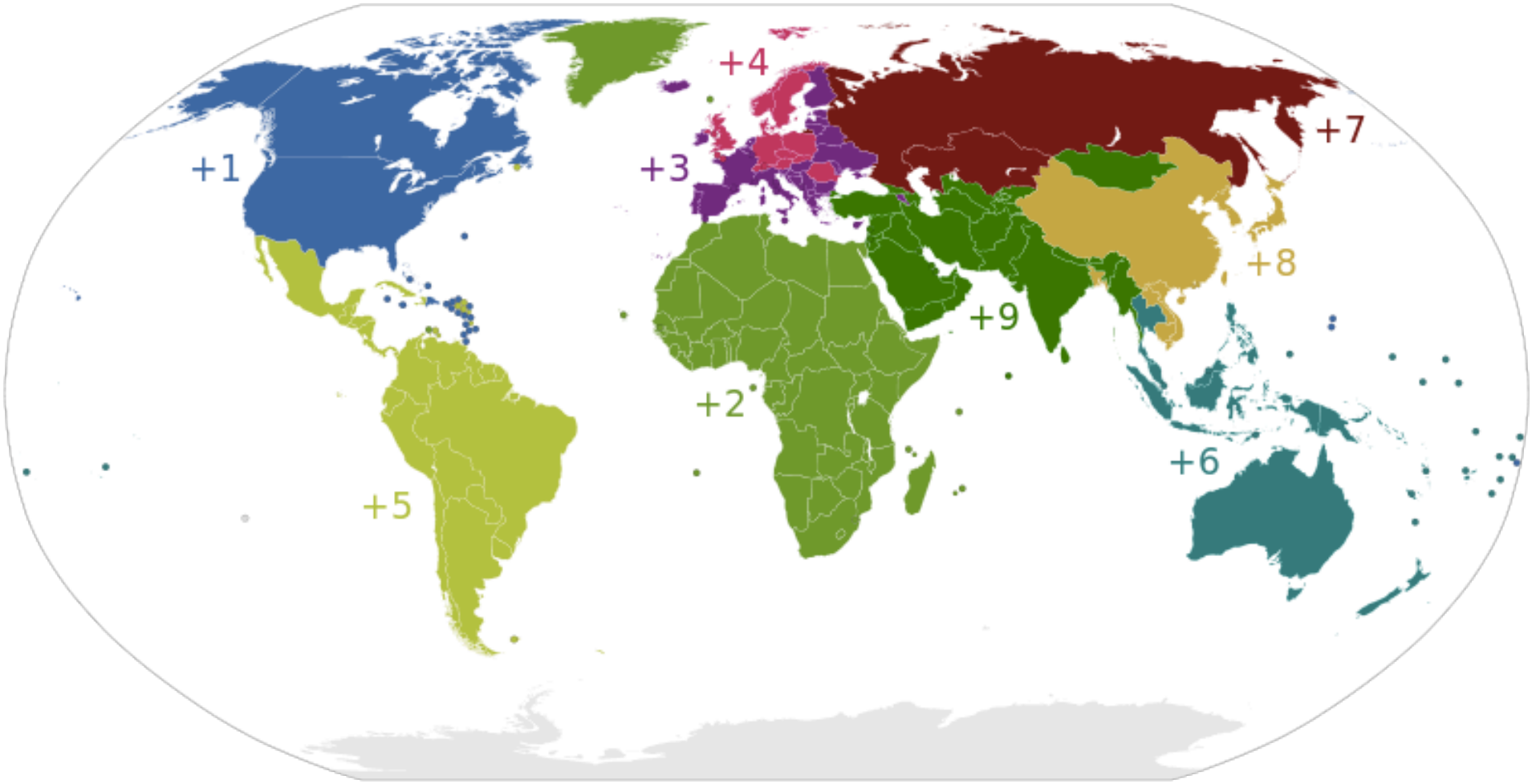

SP
SP
SP
registrars
(authorized)
add, modify,
delete
"MODB(s)"
212 555 1234 →
{x,y,z}
query
and push
ENUM
TCAP
standardized
& proprietary
APIs
ELEP
(law
enforcement)
history

State transitions

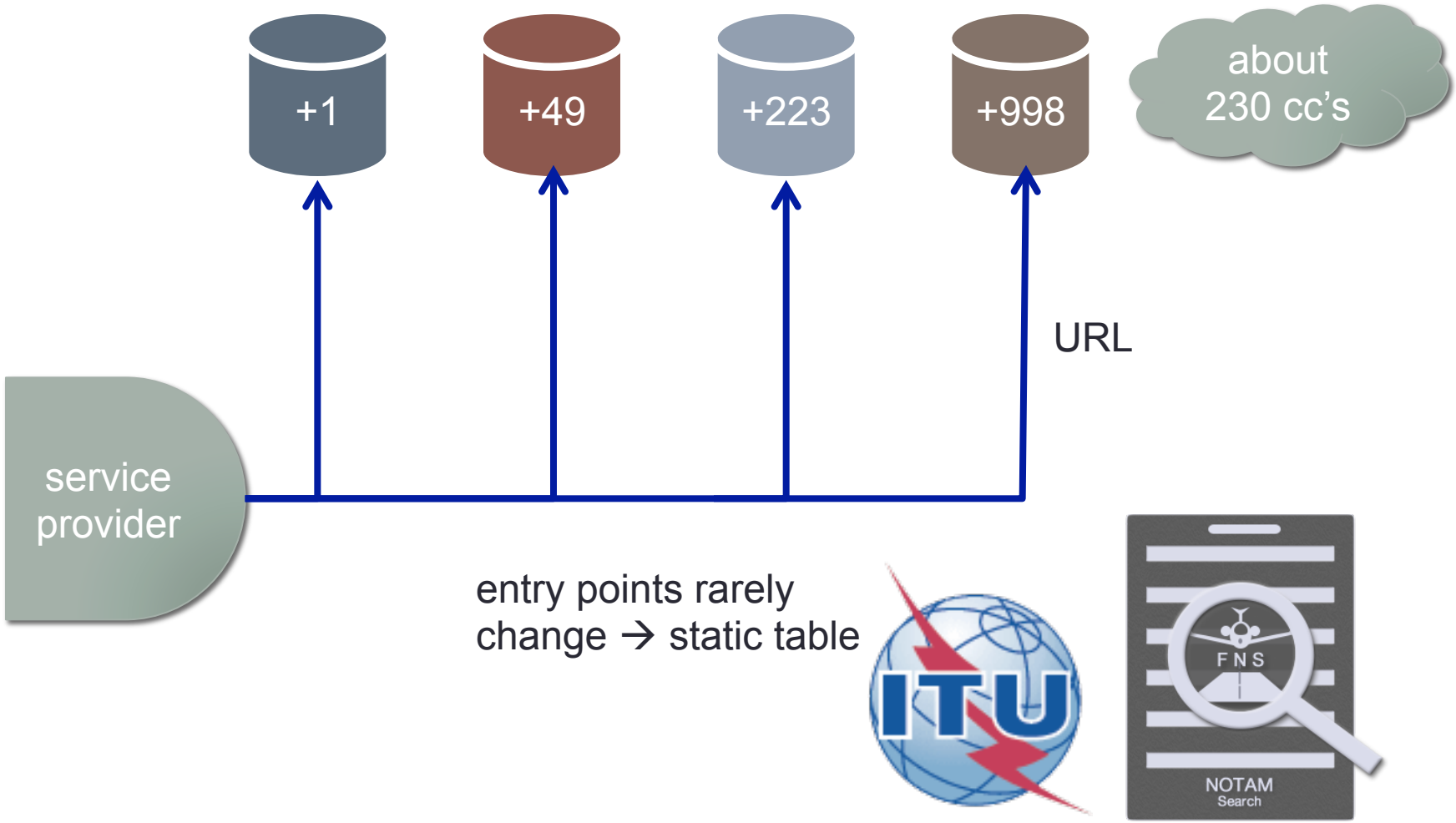


800#: Spare, Reserved, Working, Transitional, Disconnect
domain names: expired, redemption grace period (RGP), pending delete

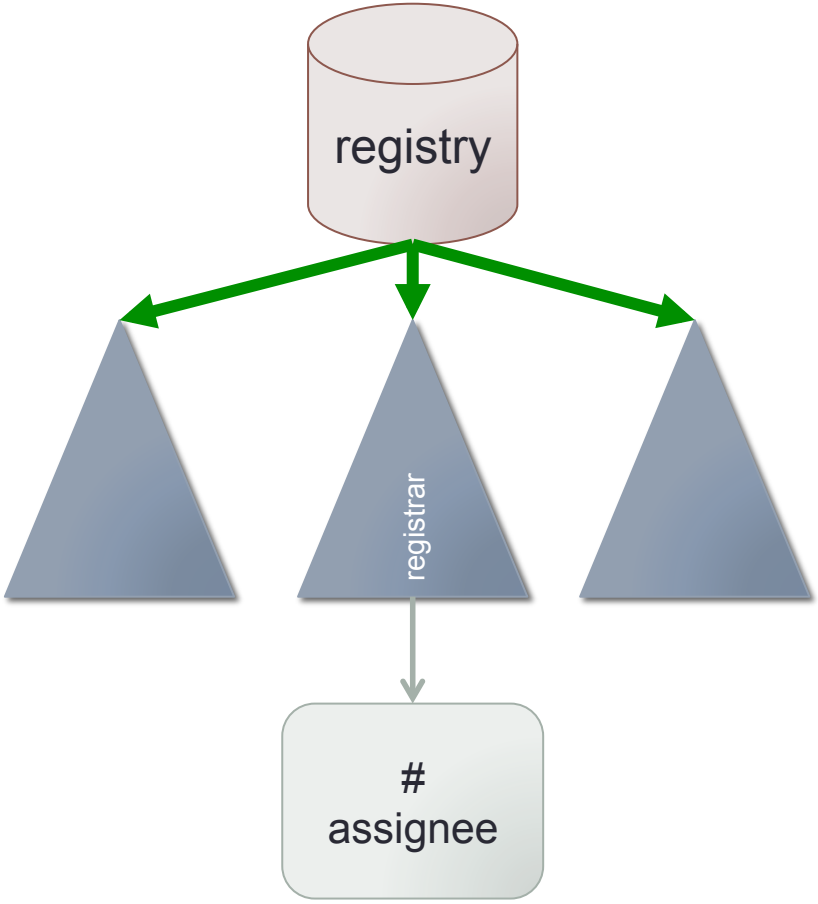
Country dialing codes



International routing



Architecture 1: tree



Architecture 2: mesh + tree

global time

registry

registry

registry

registry

assumed to be cooperative
example: TV whitespace DB, LoST (NG911)

registrar

assignee

- everybody has same information
- same state within N (7?) seconds
- revived nodes can catch up

How to ensure correctness

- Distribution of changes → gossiping
  - see LoST
- Allocation of new numbers & changes → avoid collisions
  1. block chain model
  2. Paxos, Raft and variants
     - Alice: “may I allocate number/number block X”?
     - Other nodes: “please go ahead, Alice” → quorum
     - Alice: “please change property Y of X to V”
     - Other nodes: “done”
- Recovery
  - new or revived replicas can catch up to changes
    - transaction log
    - relatively easy with timestamps (“tell me about changes after T”)

Paxos (& similar) assumptions

- Processors
  - … operate at arbitrary speed.
  - … may experience failures.
  - … with stable storage may re-join the protocol after failures (following a crash-recovery failure model).
  - … do not collude, lie, or otherwise attempt to subvert the protocol (non-byzantine)
- Network
  - Processors can send messages to any other processor.
  - Messages are sent asynchronously and may take arbitrarily long to deliver.
  - Messages may be lost, reordered, or duplicated.
  - Messages are delivered without corruption.
- A consensus algorithm can make progress using 2F+1 processors despite the simultaneous failure of any F processors.

Paxos & variants

- In order to guarantee safety, Paxos defines three safety properties and ensures they are always held, regardless of the pattern of failures:
- Non-triviality
  - Only proposed values can be learned.
- Safety
  - At most one value can be learned (i.e., two different learners cannot learn different values).
- Liveness(C;L)
  - If value C has been proposed, then eventually learner L will learn some value (if sufficient processes remain non-faulty).

Record granularity

- (1) Single record for each number
- (2) Split records by
  - geography → separate carrier by NPA or geographic region?
    - allow geographic splitting of 800#
  - service → separate carriers for audio, video, text, …
- (3) Others?

Number meta-data (examples)

Data element	Comments
E.164 number	**key**
OCN	several for different media & geographic scope?
URL	routing URL
Expiration date	if records expire
Type of number	mobile, landline (TCPA), prison, hotel
Rough location	e.g., ZIP+4 (for 311)
Public key	for STIR
whois record	similar to domain name?
Log entries (who, what, when)	need to be visible?
?	

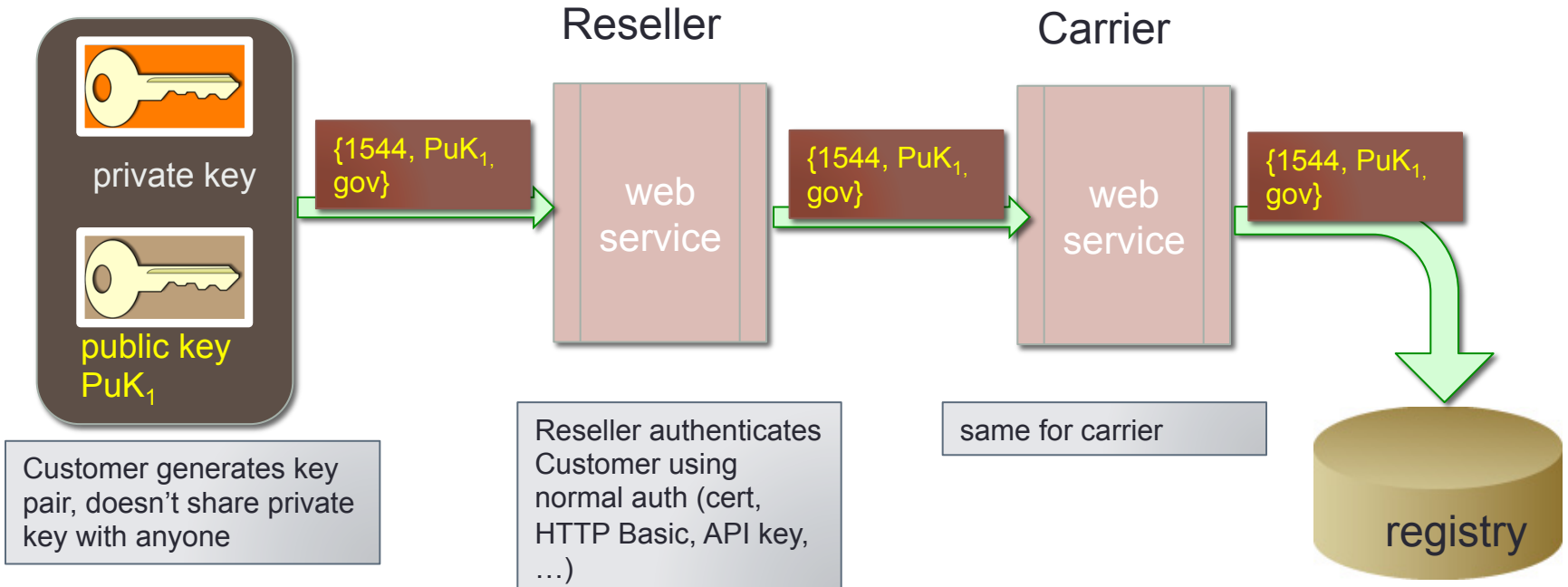
most optional

LERG

iconectiv™ experience performance results

- Operating Company Numbers, Company Names, Routing Contacts
- Country Code Assignments
- NPA Information (i.e., Area Codes)
- LATA Codes By Region
- Destination Codes (i.e., NPA NXX and Thousands-Blocks) (details on over 750,000 assignments)
- Oddball NXXs (e.g. 911, 976)
- Switching Entity Record detail (e.g. Equipment Type, V&H Coordinates)
- Rate Center details (e.g. V&H Coordinates) and Localities (including county and postal codes)
- Switch Homing Arrangements (tandem and other switch-to-switch interconnections)
- Operator Access Tandem Codes (ATCs)
- Location Routing Numbers (LRNs)

Validation: assignment with delegation



similar for certificate → CSR

Number	PuK	Prop
202 418 1544	PuK_1	.gov
212 939 7042	PuK_2	.edu

Role of caller location in numbering

- 800# allow location-specific (shared) use
- Does the architecture need to support this?
- At what granularity?
- Can this be used to simplify nationwide 211, 311 & 511?

Data elements

- Define core elements based on demonstrated need
- IANA registration for additional widely-used elements
- Possibility for OID-like or Java-like registration of private name spaces
  - `1.3.6.1.4.1.5518`
  - `edu.cmu.cs.bovik.cheese`

Whois record

- Domain names
  - creation, expiration dates
- Registrant (assignee) information
- Contacts: tech, billing, admin
- Name server information → NS record
- Currently, retrieved by simple TCP request → RDAP
  - RESTful + JSON

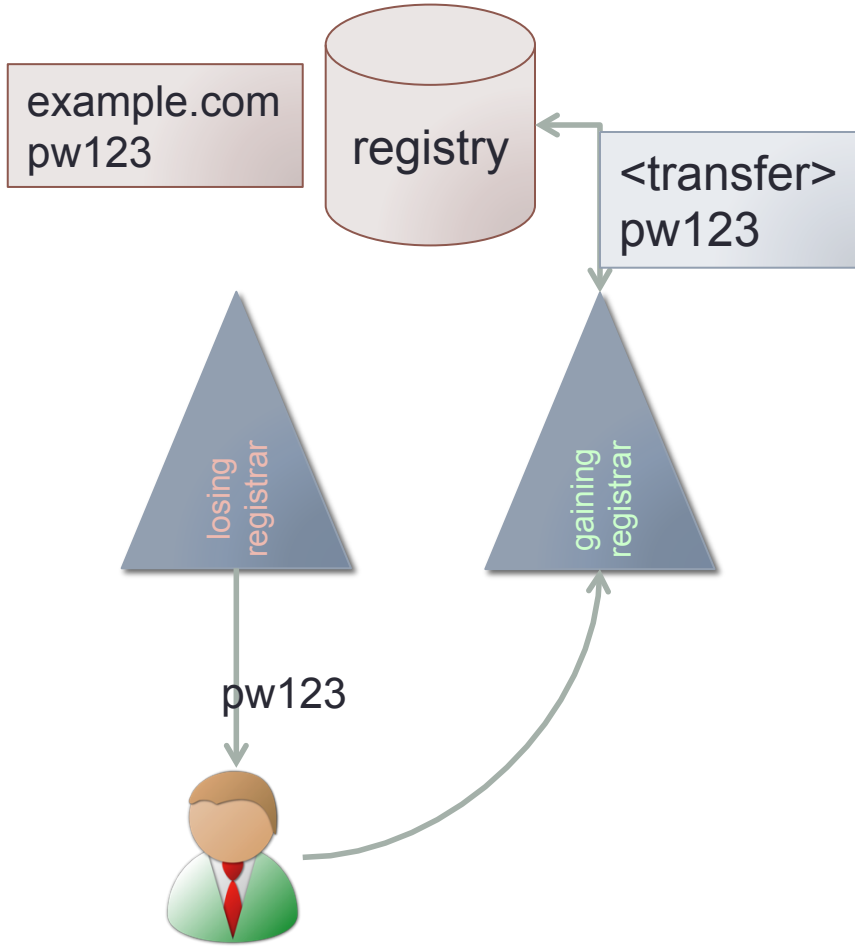
Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email@registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER[1]
Domain Status: clientDeleteProhibited[2]
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Registry Registrant ID: 5372808-ERL[3]
Registrant Name: EXAMPLE REGISTRANT[4]
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP[5]
Registrant Postal Code: A1A1A1[6]
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234[7]
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Registry Admin ID: 5372809-ERL[8]
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1

Record access model

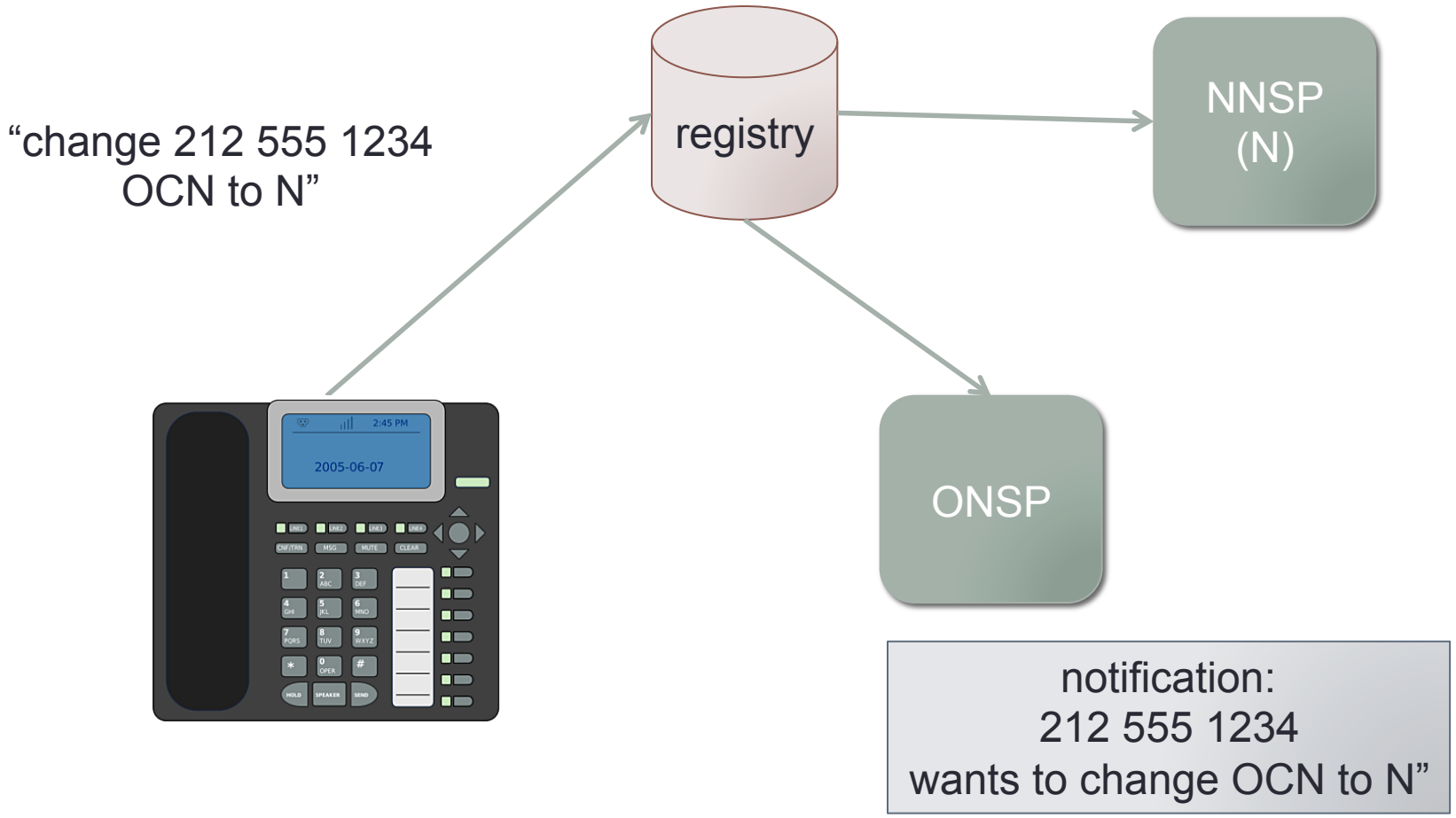
- Authorized holder (OCN) of record can modify
- through any of the registries
  - avoids dependence on any single entity
  - validated by registry
- Exception: number port → OCN change

Number porting models: token

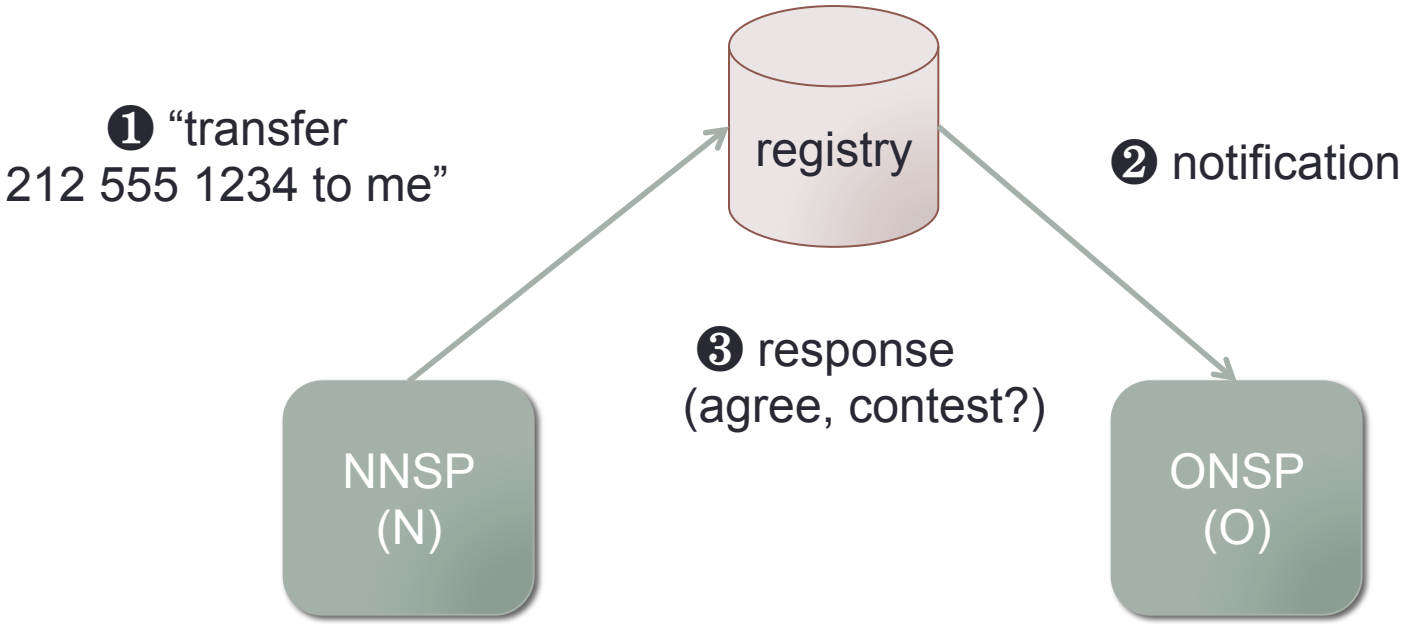
- Transfer:
  - *registrar 1 → registrar 2*
- *Porting:*
  - *provider 1 → provider 2* (in EPP, that's an **<update>**)
- Token model ("AuthInfo" in EPP)
  - current registrar provides secret token to assignee
    - or assignee inserts random token via registrar
  - assignee provides token to gaining registrar/carrier
  - Oauth bearer token (RFC 6750)?



Porting: end user initiated



Porting: confirmation-based



Protocol ops: allocation

- Example: EPP operations (RFC 5730, 5731)
  - ENUM: RFC 4114
  - separate “contact” definition
- EPP operations
  - session **<login>**, **<logout>**
  - query **<check>, <info>, <poll>, <transfer>**
  - object **<create>, <delete>, <renew>, <transfer>, <update>**
- Additional authorization via HTTPS client certs or similar?
- *What can we learn from EPP?*

Porting: other models

- Add neutral third party (TPV)
  - gaining registrar/carrier transfers request to neutral 3rd party
  - 3rd party validates request
  - passes validated request to carrier (registrar? registry?)
- User certificate: sign transfer request
- OAuth
- Others?

Caching

- Caching can improve performance and increase resiliency
- But: porting and other change events need to be visible quickly
  - how quickly – seconds? minutes? hours?
  - 1.48 million porting events / day (10% user-initiated)
    - ➔ 1.7 user events/second or (roughly) 136 bps
    - very roughly 0.1% of all assigned numbers
- Caching approaches:
  - **Passive**: explicit expiration time
  - **Active**: publish-subscribe notification of registrars and other entities for numbers they care about → cache invalidation
    - can “push” cache invalidation scale?

Fair assumptions?

- JSON (or XML?) over HTTPS, REST-style
- Do we need any pub/sub mechanism?

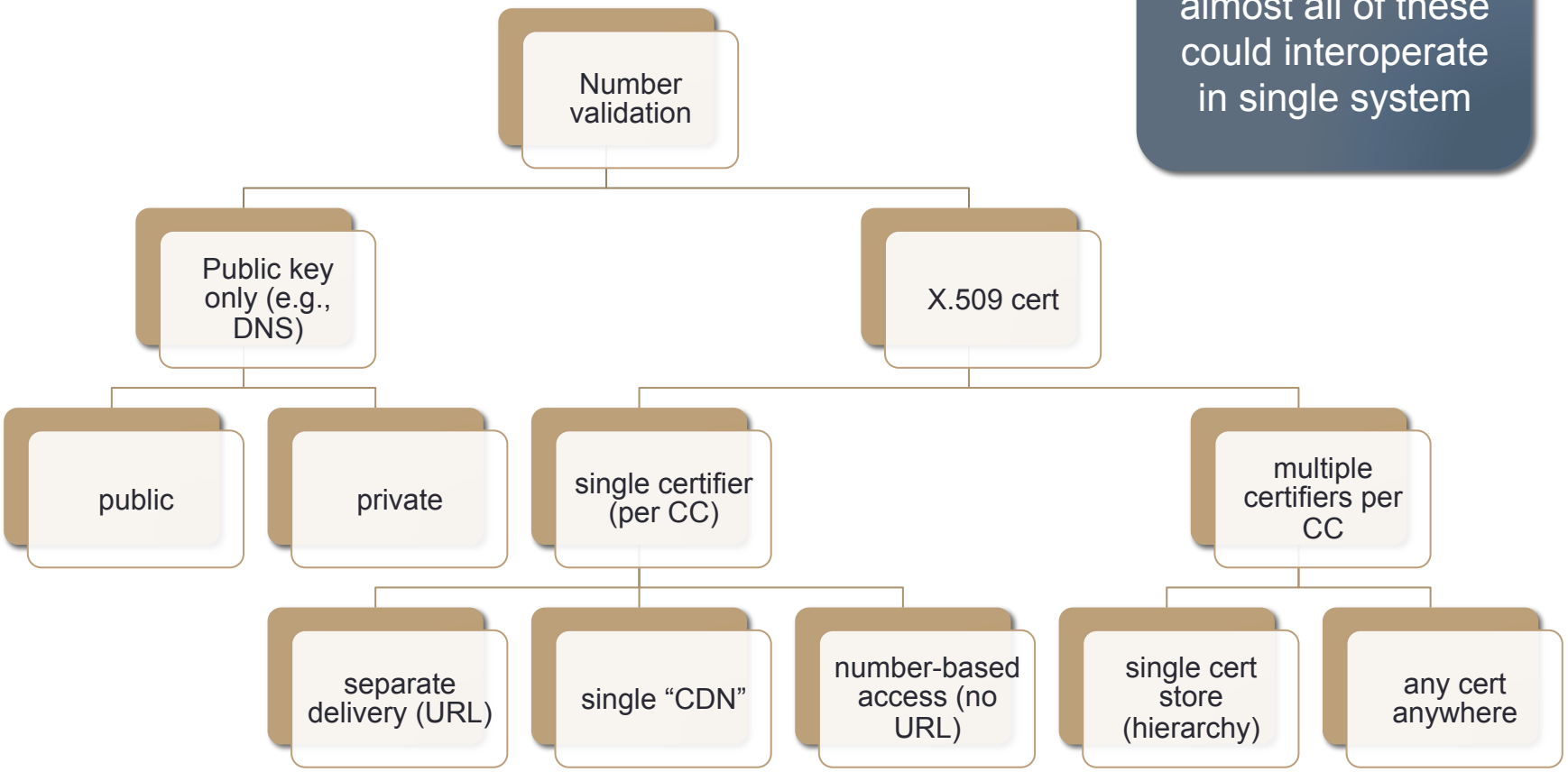
Open issues (selection)

- Architectures (tree, mesh, …)
- State transitions and process flows – can they be abstracted so that other entities can write profiles?
- Data model: plain I-JSON, YANG, …
- Protocols to learn from (or use): EPP, ENUM, RDAP, YANG, …
- Read queries: number → data elements
- Update (& synchronization) queries

BACKUP

Key management options

almost all of these could interoperate in single system



Certificate models

- *Integrated* with number assignment
  - assignment of number includes certificate: “public key X is authorized to use number N”
  - issued by number assignment authority (e.g., NPAC), possibly with delegation chain
    - allocation entity → carrier (→ end user)
- *separate* proof of ownership
  - similar to web domain validation
  - e.g., similar to Google voice validation by automated call back
    - “Enter the number you heard in web form”
  - Automate by SIP OPTIONS message response?

EPP Command Example

```
<?xml version="1.0" standalone="no"?>
<epp xmlns="urn:iana:xmlns:epp"
     xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
     xsi:schemaLocation="urn:iana:xmlns:epp epp.xsd">
  <command>
    <ping>
      <domain:ping xmlns:domain="urn:iana:xmlns:domain"
       xsi:schemaLocation="urn:iana:xmlns:domain domain.xsd">
        <domain:name>example1.com</domain:name>
        <domain:name>example2.com</domain:name>
        <domain:name>example3.com</domain:name>
      </domain:ping>
    </ping>
    <trans-id>
      <date>2000-06-08</date>
      <client-id>ClientX</client-id>
      <code>ABC-12345-XYZ</code>
    </trans-id>
  </command>
</epp>
```

EPP Response Example

```
<?xml version="1.0" standalone="no"?>
<epp xmlns="urn:iana:xmlns:epp"
     xmlns:xsi="http://www.w3.org/1999/XMLSchema-instance"
     xsi:schemaLocation="urn:iana:xmlns:epp epp.xsd">
  <response>
    <result code="1000">
      <text>Command completed successfully</text>
    </result>
    <response-data>
      <domain:ping-data xmlns:domain="urn:iana:xmlns:domain"
       xsi:schemaLocation="urn:iana:xmlns:domain domain.xsd">
        <domain:name result="known">example1.com</domain:name>
        <domain:name result="unknown">example2.com</domain:name>
        <domain:name result="known">example3.com</domain:name>
      </domain:ping-data>
    </response-data>
    <trans-id>
      <date>2000-06-08</date>
      <client-id>ClientX</client-id>
      <code>ABC-12345-XYZ</code>
    </trans-id>
  </response>
</epp>
```