



The GNU Name System

Bernd Fix, Christian Grothoff, **Martin Schanzenbach**

2023-09-27

Label
www.example.com
Namespace



The diagram illustrates the components of the domain 'www.example.com'. A bracket above the text 'www' is labeled 'Label'. A bracket below the text '.example.com' is labeled 'Namespace'.

The .alt TLD

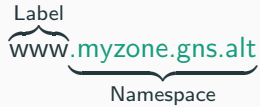
Whats wrong with DNS? See RFC 8324¹:

- No **query privacy**.
- A **single hierarchy with a centrally controlled root**.
- Requires management/maintenance of **root servers**.
- etc. . .

DNSSEC and other “patches” do not or in adequately address the issues: “[the existing solutions for DNS are] security patches rather than designed-in security or privacy mechanisms”.

¹DNS Privacy, Authorization, Special Uses, Encoding, Characters, Matching, and Root Structure: Time for Another Look?

Label
www.myzone.gns.alt
Namespace



The .alt TLD

Why “.gns.alt”?

- RFC9476: “The .alt Special-Use Top-Level Domain” defines the TLD to be used for alternative (from the point of view of DNS) name systems.
- RFC9476 does **not** define a registry for “.alt”-subdomains.
- We manage a “.alt” registry at <https://gana.gnunet.org>² which already includes a code point for “.gns.alt”.
- To prevent shadowing of DNS names, it is recommended to use the “.gns.alt” suffix.
- Sometimes (e.g. censorship-overrides) you may not want to do that.

²If you ever need a registry for your protocol feel free to approach us!

The GNU Name System

- Namespaces are created and uniquely identified using **public zone keys**.
- Records** are grouped by **label**, encrypted, signed, and published in a key-value store (usually, a DHT³).
- Supported zone types and crypto (for now):
 - PKEY: ECDSA+CTR-AES-256
 - EDKEY: EdDSA+XSalsa20-Poly1305


Private Key

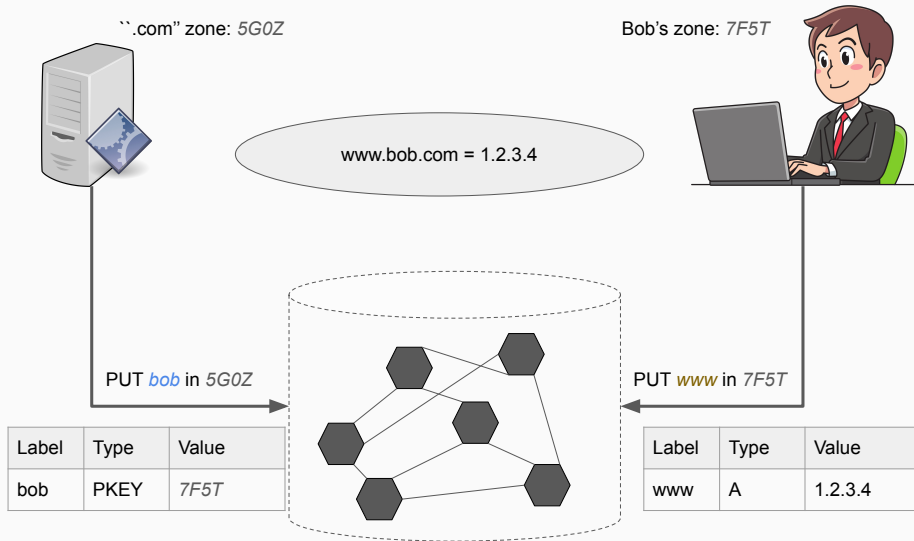

Public Zone Key

Label

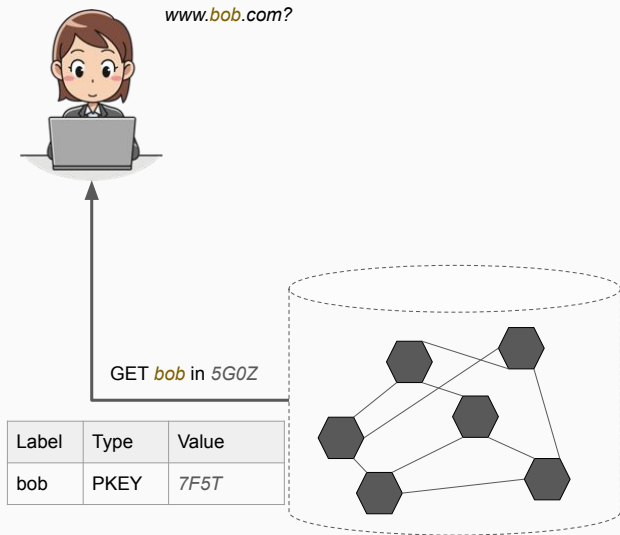
Resource Records
A: 1.2.3.4 TXT: Hello World MX: mail.example.org

³<https://datatracker.ietf.org/doc/draft-schanzen-r5n/>

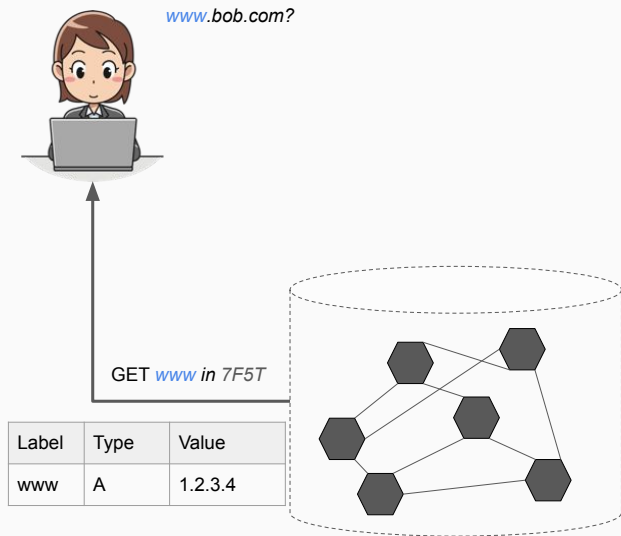
Zone management



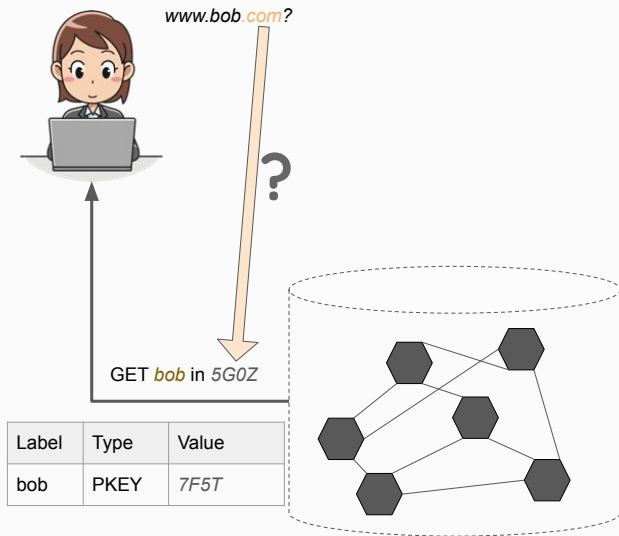
Name resolution



Name resolution



How do we bootstrap the top-level zones?



“Hyper-hyper local root” concept we call the **Start Zone**:

- Start Zone contains so-called **suffix-to-zone**-mappings.
- Implementation ships with an *initial* Start Zone configuration.
- Start Zone is configurable *locally* at *each* endpoint.
- User override/extension of mappings at top-level or subdomain-level for:
 - Circumvent censorship if necessary.
 - Private networks.

Example suffix-to-zone mappings:

Some TLDs

.com = 000G001MF6DVMZZ4Y8XRZQDXM1PB3D3VGEK29ZHXBA57EPSNW1QBPKT8J0

.myzone.gns.alt = 000G007FKSA876G6SNDF8VA7YK1DJE96RPPBHRT2X55Q13M2T4YKNYT3DG

Some subdomain overrides

.gnu.org = 000G001223Q8ZJZBSK6XT2DWV6PE5B1W436D2NB7ZBR9XSXT7TFJHCDB24

.gnunet.gns.alt = 000G0047M3HN599H57MPXZK4VB59SWK4M9NRD68E1JQFY3RWAHDMKAPN30

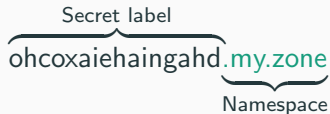
Possible Governance Models

- Non-profit organization.
- Multi-stakeholder model: Board, supporting organizations, ...
- Examples for possible stakeholders:
 - Software and OS Distributors
 - Browser vendors
 - Governments
- Funding options:
 - Applications for new top-level domains.
 - Registrations of new top-level domains.
 - ...

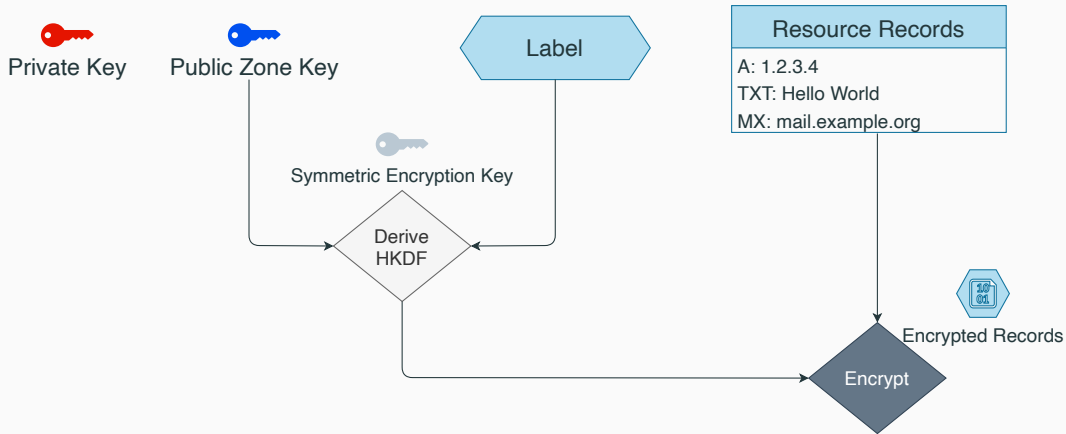
Hiding information inside GNS

- GNS's crypto allows you to hide resource records.
- It requires either
 - the use of a label with sufficient entropy (a shared secret) or
 - the use of a secret zone.

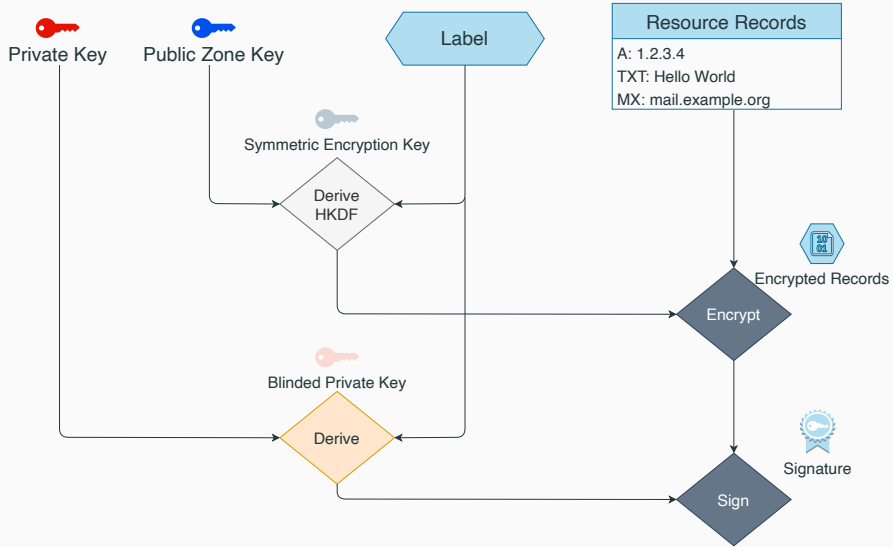
Secret label
ohcoxaiehaingahd.my.zone
Namespace

A diagram illustrating the components of a GNS label. The text "ohcoxaiehaingahd.my.zone" is shown. A curly brace above the "ohcoxaiehaingahd" part is labeled "Secret label". Another curly brace below the ".my.zone" part is labeled "Namespace".

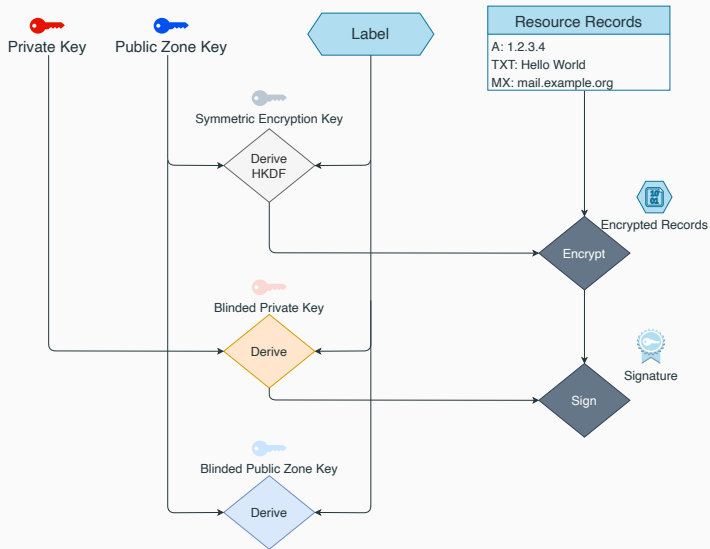
Encrypt



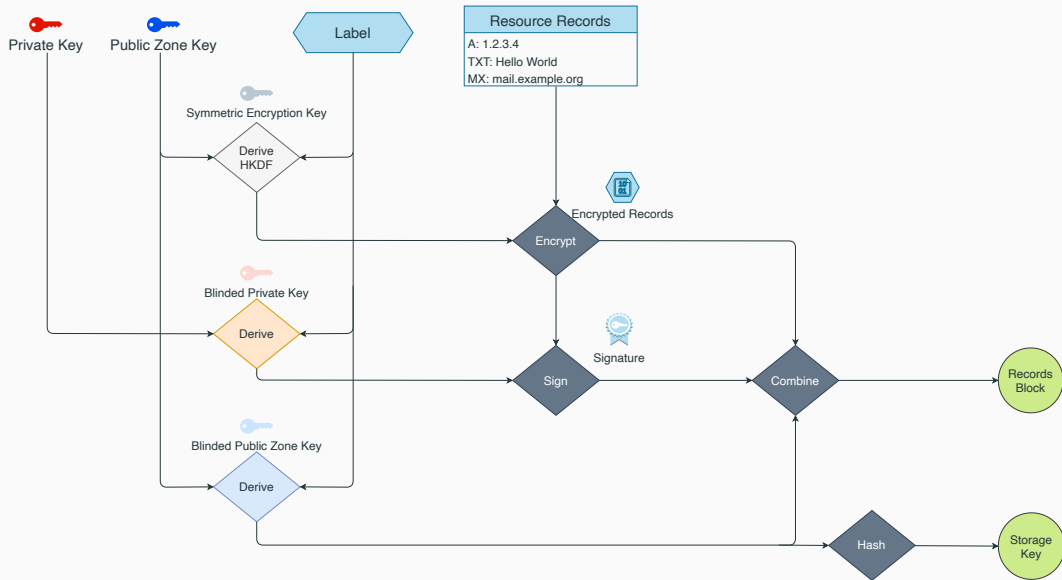
Sign



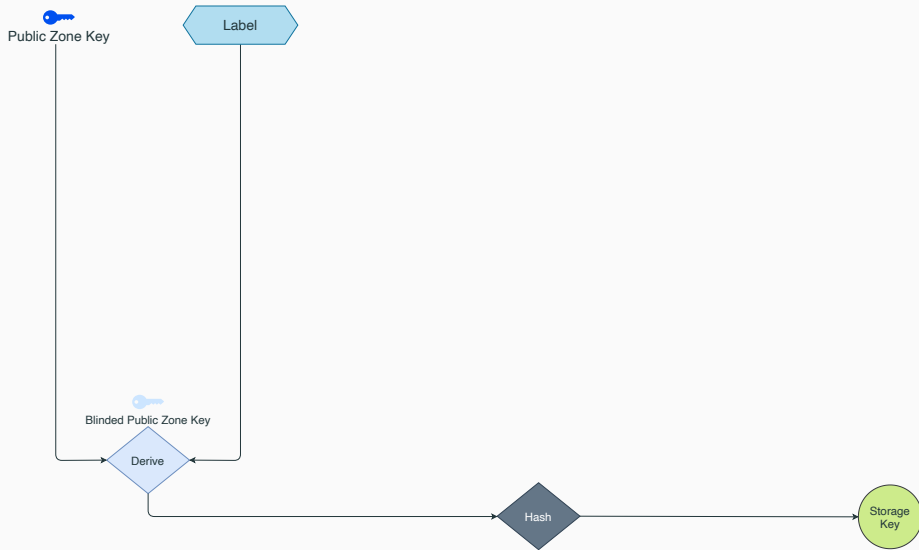
Derive



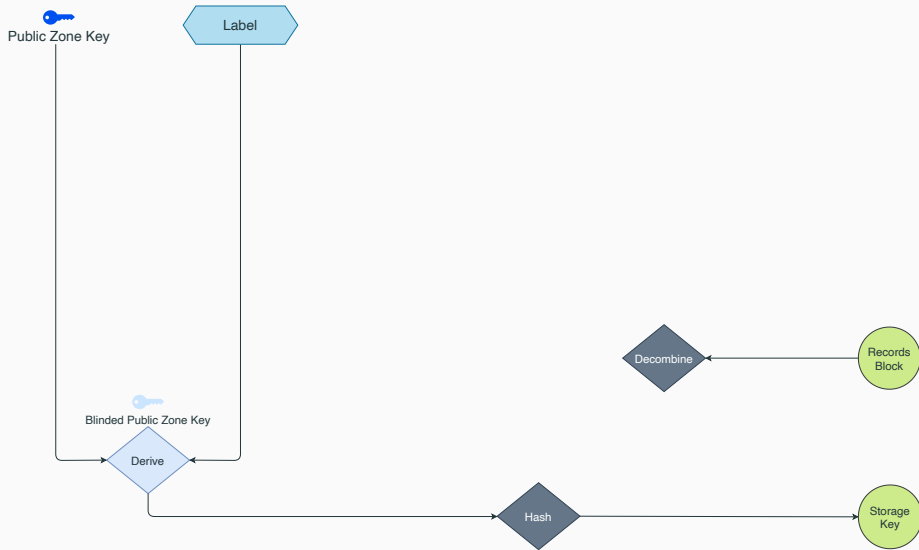
Combine and publish



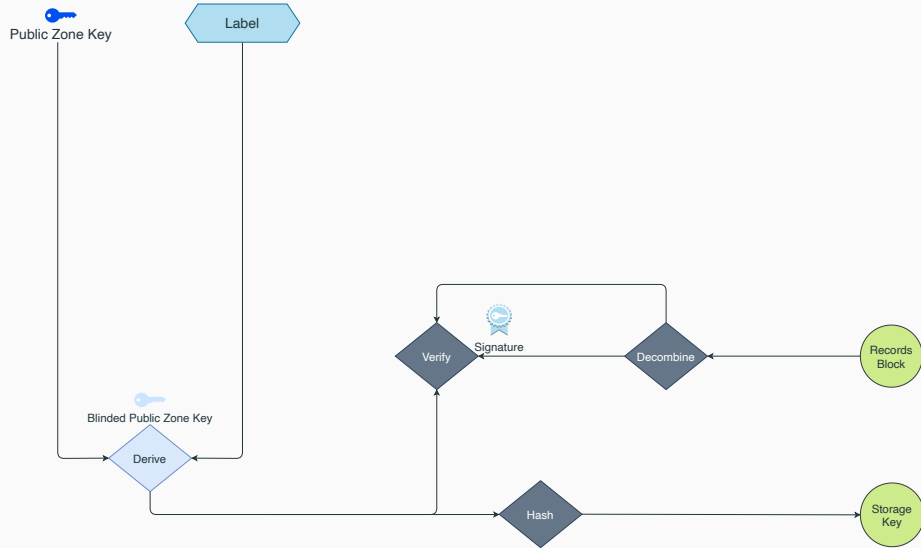
Query



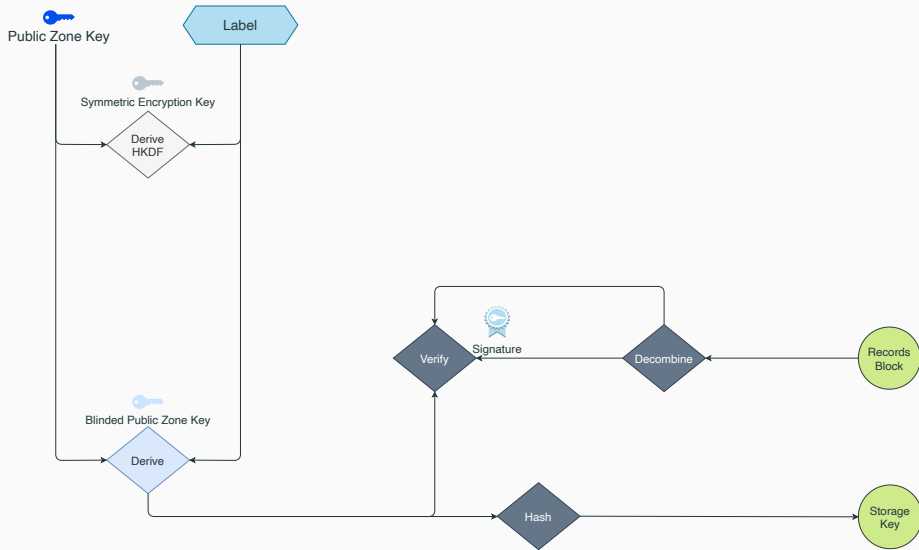
Retrieve



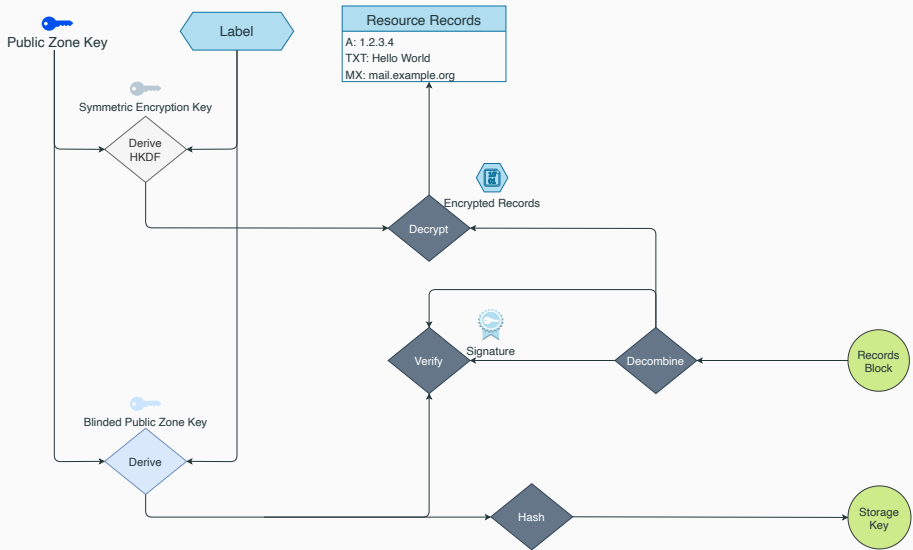
Verify



Decrypt



Decrypt



- Specification efforts:
 - <https://datatracker.ietf.org/doc/draft-schanzen-gns/> – Will become RFC soon (TM).
 - <https://datatracker.ietf.org/doc/draft-schanzen-r5n/> – Is being worked on.
- Reference implementation in C (part of GNUUnet), alternative implementation in Go.
- Currently funded project to develop and host a GNS zone registrar service and to mirror some (large) DNS zones funded through NLnet / NGI Zero Entrust.
- Current and future research:
 - PQ-secure key blinding.
 - Sharing identity information via GNS (re:claimID).

Questions?

<https://gnunet.org>

schanzen@gnu.org

3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A