

The Role of DNS Names in Internet Decentralization

Tianyuan Yu

IETF 121 DINRG

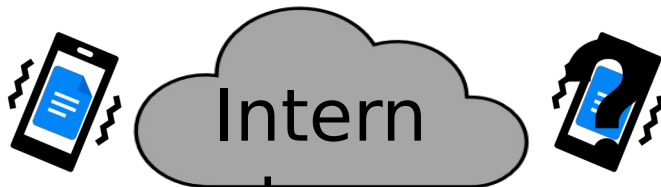
2024/11/06

What is the Issue

- (Almost) All today's user apps are provided by / running on the cloud
 - Reliance on / controlled by cloud providers
 - All user data captured by cloud providers
- One way out of this: developing a new generation of apps *controlled by* end users (instead of cloud providers)

How to Build Such New Apps

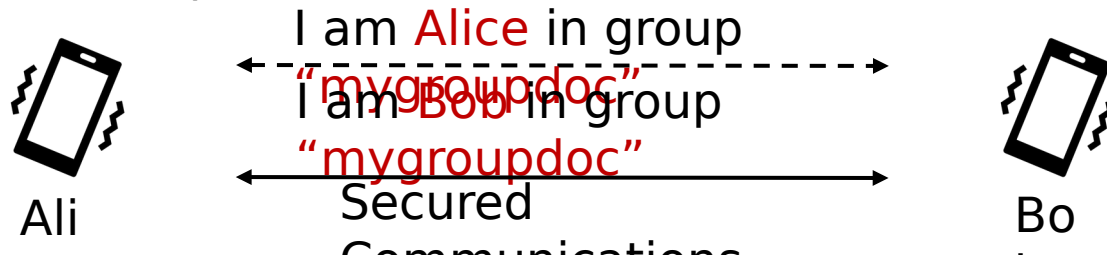
- Enabling direct, secure, user-to-user communications (U2U)
- One way to get there
 - Let users get DNS names
 - Users can then authenticate each other using standard security libraries
 - Let users authenticate each other, without reliance on external PKIs
 - Instead, use trust-policies defined by users



Bob, this is from
Alice

Why DNS names for users

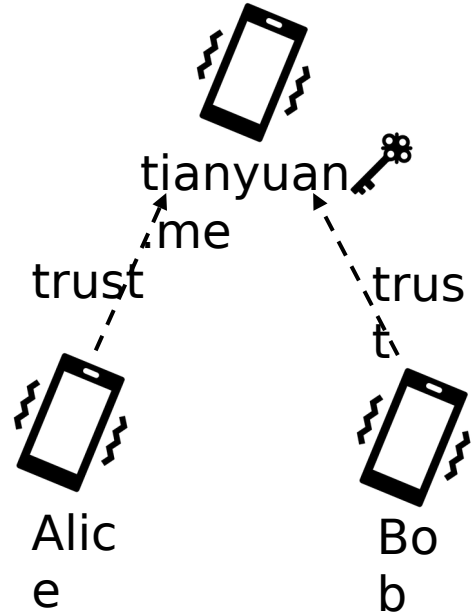
- Make usernames *independent* from cloud providers
 - alice@named-data.net, bob@named-data.net
 - Contrast to today: users are identified by their gmail address or Facebook IDs (2 companies control how all users identify themselves in cyberspace)
- Have names directly under users' control
 - DNS name delegation lets one freely create new names under one's own namespace



Establishing trust among users

- Make use of DN name delegation
 - .tianyuan.me (owner)
 - .mygroupdoc.app.tianyuan.me (app)
 - .alice.mygroupdoc.app.tianyuan.me (user)
- Users issue certs to others in the trust circle
 - Remove external reliance

A diagram showing a trust anchor. It consists of a key icon on the right labeled "Local trust anchor". To its left is a dashed line that branches into two paths. The top path leads to a red-bordered box containing ".alice" followed by a grey-bordered box containing ".mygroupdoc.app.tianyuan.me". The bottom path leads to a grey-bordered box containing ".tianyuan.me".



User named and controlled data

- Users publish named data
 - alice.mygroupdoc.app.tianyuan.me/blog/post/2024-11-06/dinrg
 - Encryption
 - Signed by alice.mygroupdoc.app.tianyuan.me key
- Rest of the story: exchange data
 - Overlay networks that communicate by names



Alice

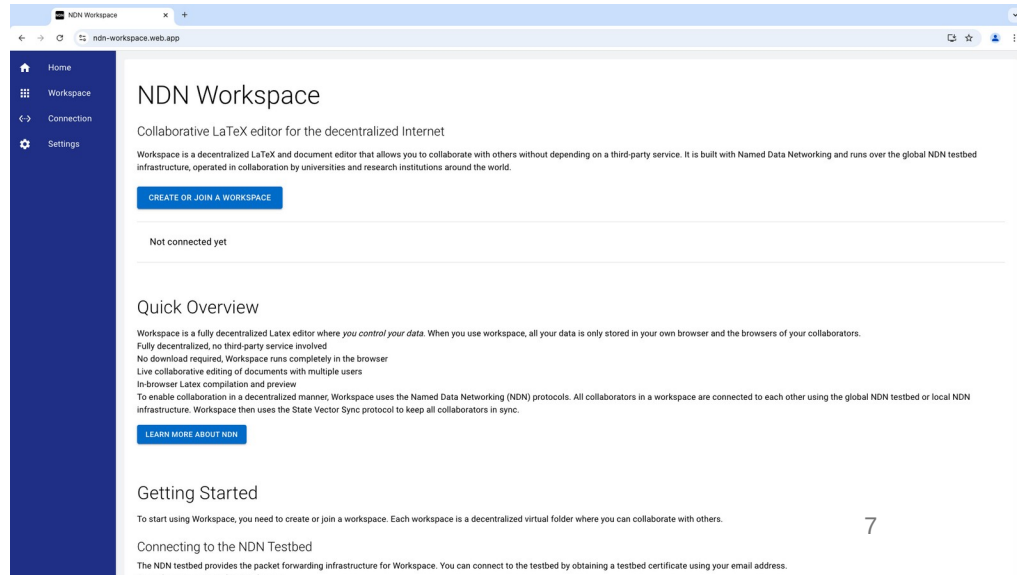
“Hey I am Alice, please propagate that I am hosting data at your place



NDN Workspace

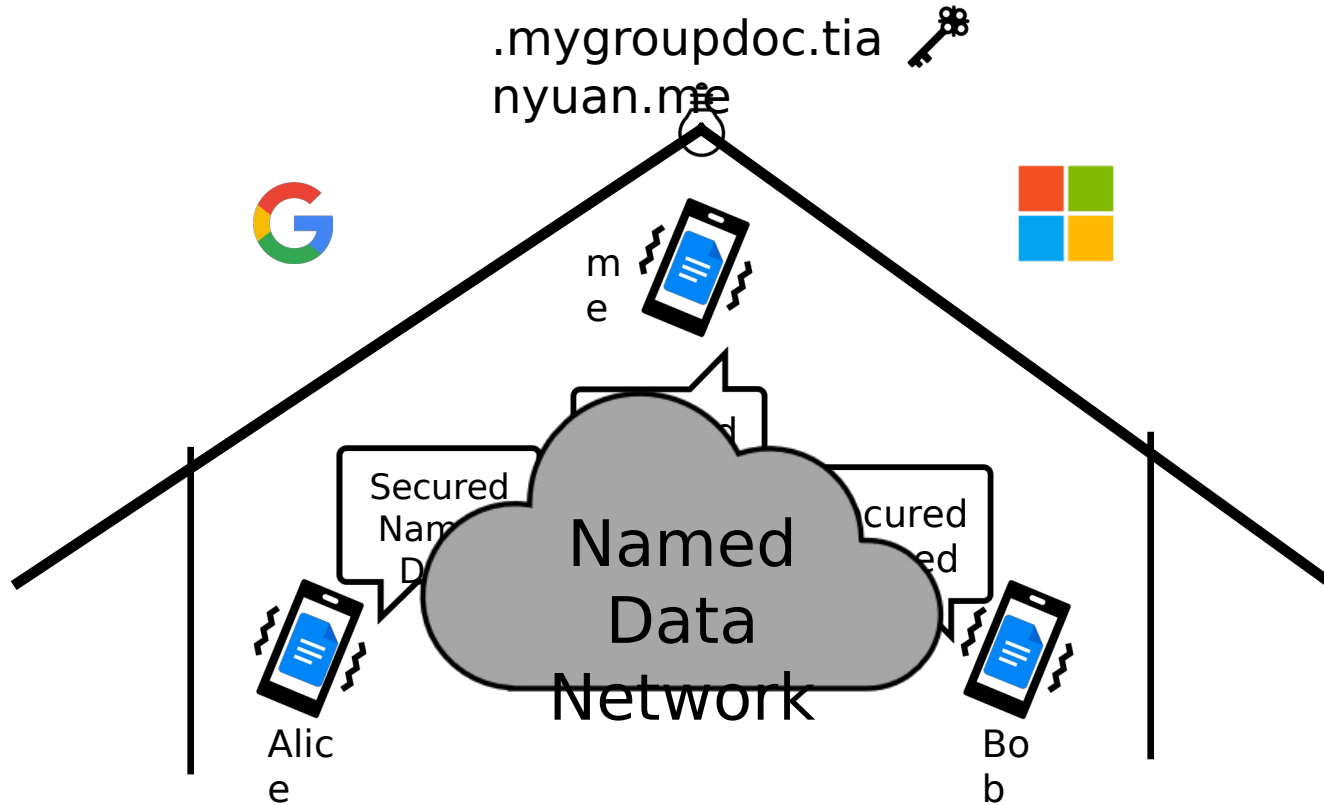
- IETF119 DINRG
 - *Workspace: Local-first Collaborative Editing over NDN*

Decentralizing control
back to users!

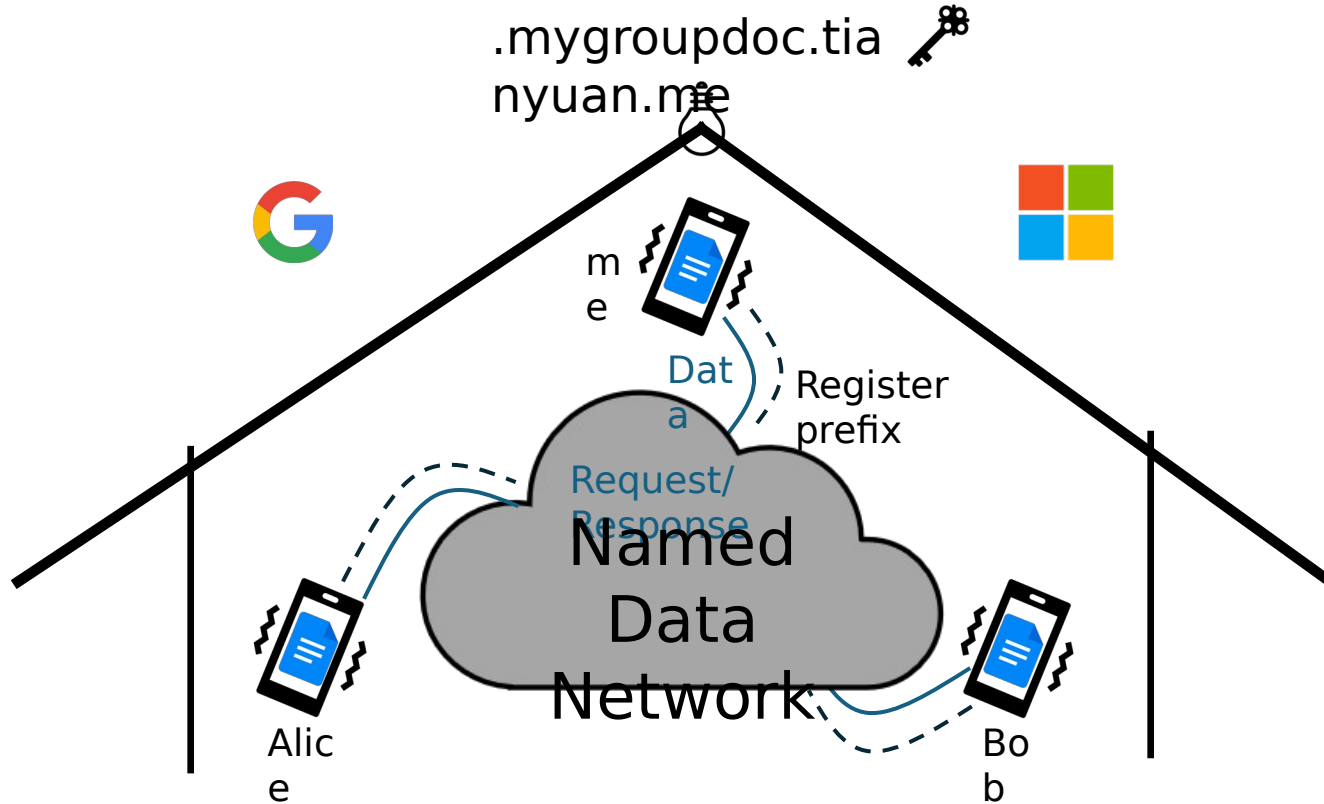


The screenshot shows the NDN Workspace web application interface. The browser address bar displays "ndn-workspace.web.app". A dark blue sidebar on the left contains navigation links: Home, Workspace, Connection, and Settings. The main content area features the title "NDN Workspace" and a subtitle "Collaborative LaTeX editor for the decentralized Internet". Below this, a paragraph explains that the workspace is a decentralized LaTeX and document editor built with Named Data Networking (NDN) protocols. A prominent blue button labeled "CREATE OR JOIN A WORKSPACE" is visible. The status indicates "Not connected yet". A "Quick Overview" section follows, detailing that the workspace is fully decentralized, requires no download, and supports live collaborative editing. A "Getting Started" section begins with the instruction to create or join a workspace. The page number "7" is located in the bottom right corner.

Workspace: A Local-First App Prototype



Workspace: A Local-First App Prototype

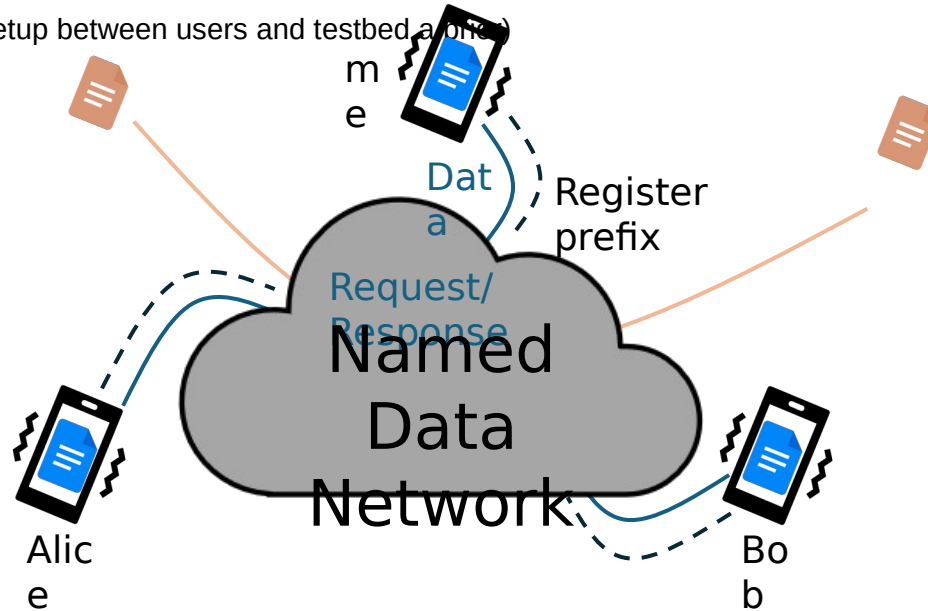


Communication over the Public Internet

- NDN Testbed

- an overlay, NDN-speaking nodes connected by tunnels (with its own trust anchor)
- Accepting routing announcements after authenticating the name prefix ownership

(trust relation setup between users and testbed a one)



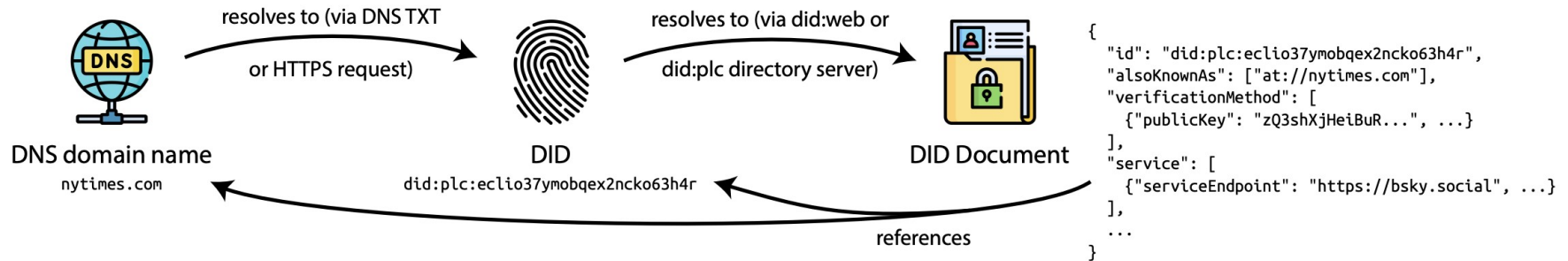
Giving DNS Names to End-users

- Shared idea with multiple other efforts
 - DANE Authentication for Network Clients Everywhere (DANCE)
 - TLS clients with X.509 certificate
 - draft-ietf-dance-architecture-07
 - 4.1.7 Domain users
 - “Domains who publish TLSA records for a CA under a _user name underneath their domain allow the validation of user identities as mentioned in a certificate as TLS client or peer identities.”*

Another Use Case Along the Same Direction

- Bluesky 

- Binding a Decentralized Identity (DID) to a DNS name



The Trend of Moving Toward Name-based Networking

A new Internet Architecture

- We've moved from end-to-end peer networks to client/server asymmetric networks
 - We've replaced single servers with replicated servers
 - Clients are identified with a unique public IP address – clients are uniquely identified only in a local context
 - Individual services aren't identified with a unique public IP address – services are identified in the DNS
- We've moved from address-based networks to name-based services*

Naming in Networking

- Naming is the first and most important thing in networking
 - Host name, service name, data name, username, etc.
- Networking today is based on DNS names (albert at higher level)
- Giving users DNS names enables direct U2U (assisted by name-based forwarding), which enables user-controlled apps, an effective step walking away from further centralization