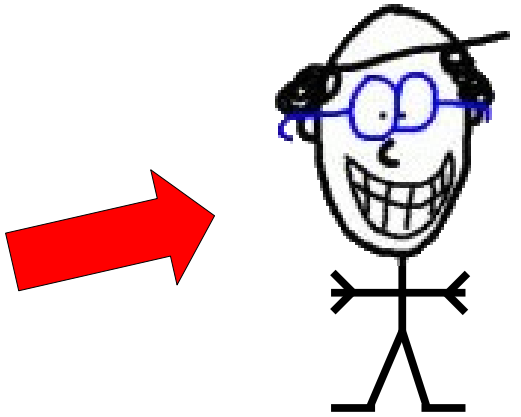
Verifiable **I**dentity using **D**istributed **A**uthentication (VIDA)

Dr. Neal Krawetz
Hacker Factor



Problem Space

- Need reliable way to attribute content to author

  “Is it authentic?”

  “Was it altered?”

  “Who created this?”

  - False attribution
  - Non-repudiation

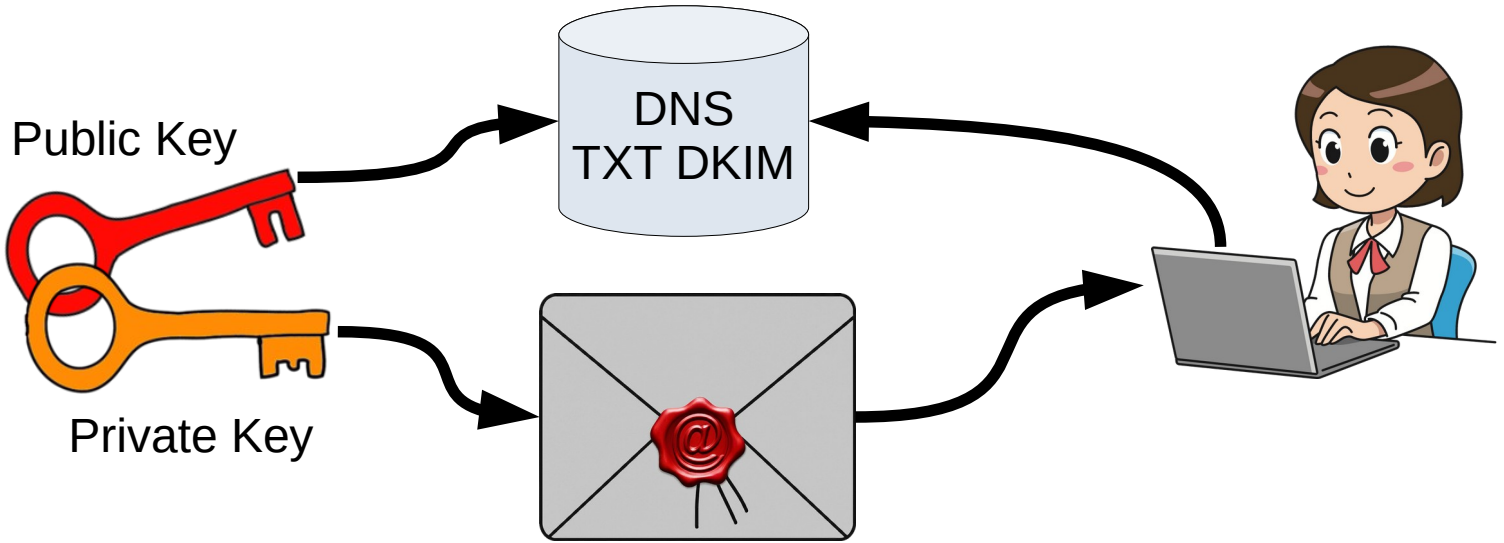
Existing Proposed Solutions

- Blockchain
  - Fails to scale to high volume
  - Many use proprietary details

- C2PA (Content Coalition for Provenance and Authentication)
  - Corporate-driven solution, closed-door design
  - 100% based on “trust”
    - Trust metadata & content is legitimate
    - Trivial to make cryptically authenticated forgeries
  - Pay to Play (no self-signed X.509 certs)

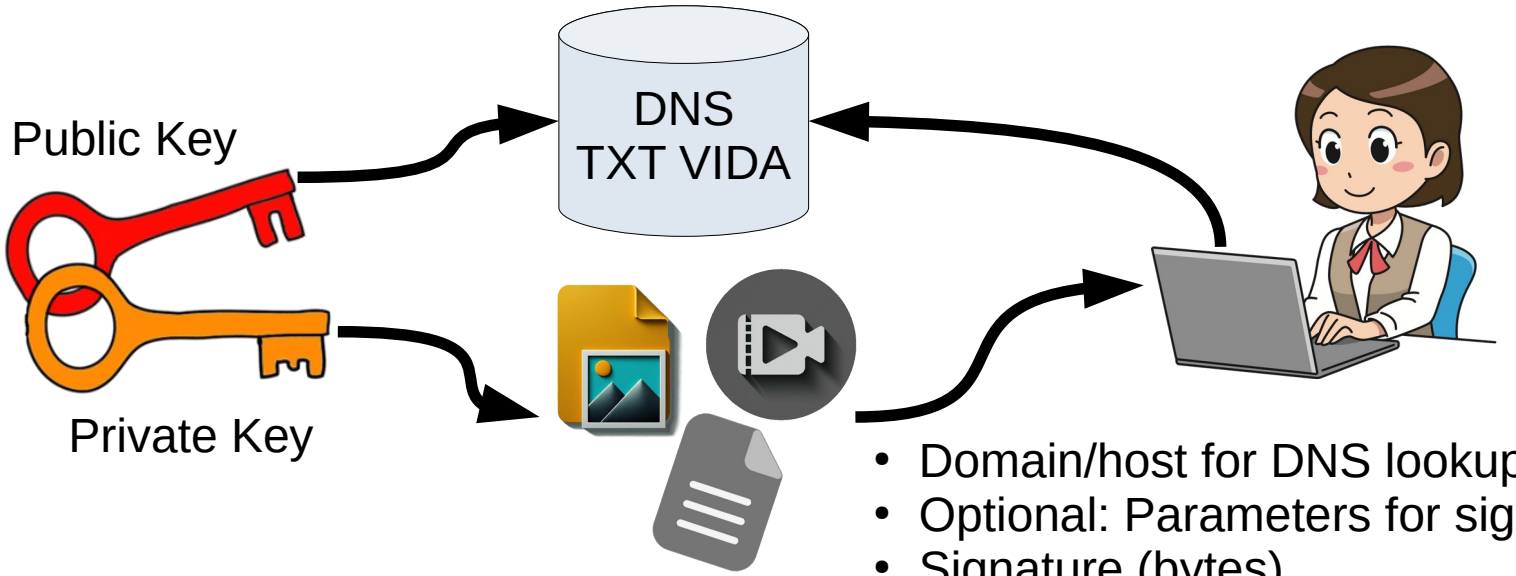
Proposed Solution

- Anti-Spam got it right!
  - DKIM (RFC 6376, DomainKeys Identified Mail)



Proposed Solution

- VIDA: validation based on DKIM



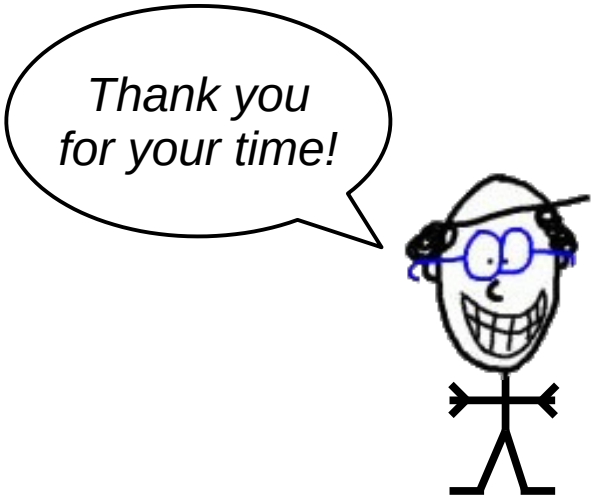
VIDA Provides

Attribution	Attributed to the domain or hostname
Authentication	It came from the domain; private key prevents forgeries
Validation	Cryptographic signature identifies tampering
Non-repudiation	Only your domain has private key, so it came from your domain!
Low cost	Domain required, but permits signing services! (Cheaper than X.509)
Privacy	DNS relays, no centralized validator, signer cannot track usage
Distributed	DNS! Anyone can use this; no dependency on single vendor

What I Need...

- Help!
  - Ironing out specification details
  - Writing up the RFC
    - Navigating the RFC submission process
    - Reducing my long essays to minimal RFC documentation
  - Implementing
    - Working examples and public tools/libraries

Verifiable **I**dentity using **D**istributed **A**uthentication (VIDA)



Contact:

Dr. Neal Krawetz
Hacker Factor
pasta@hackerfactor.com