Bern University of Applied Sciences

IARIA

Verifiable Labels for Digital Services: A Practical Approach

Authors: Maël Gassmann, Annett Laube
Presenter:
Maël Gassmann
Institute for Data Applications and Security
Email: mael.gassmann@bfh.ch

About me - Maël Gassmann

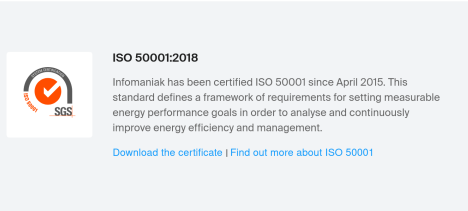
- Swiss
- French native speaker; German
- BSc in Computer Science in 2022 at the BFH
- MSc in Engineering 2^{nd} semester at the BFH
- 50% Assistant in the BFH's Institute for Data Applications and Security

Summary

1. Introduction
2. State of the Art
3. Concept
4. Implementation
5. Conclusion

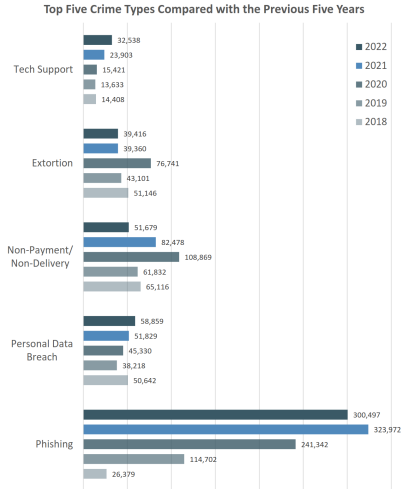
Introduction

- Digital graphical representations
  - Electronic documents, pictures
- Easy to copy
- Equivalent to self-proclamation
- Hard and inconvenient (if not impossible) to verify
- Problem:
  - Some people give it value
  - It hardly has any actual value



https://infomaniak.com/en/certifications

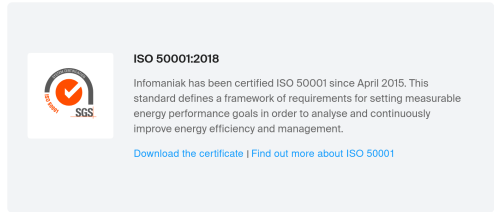
Introduction



https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Introduction

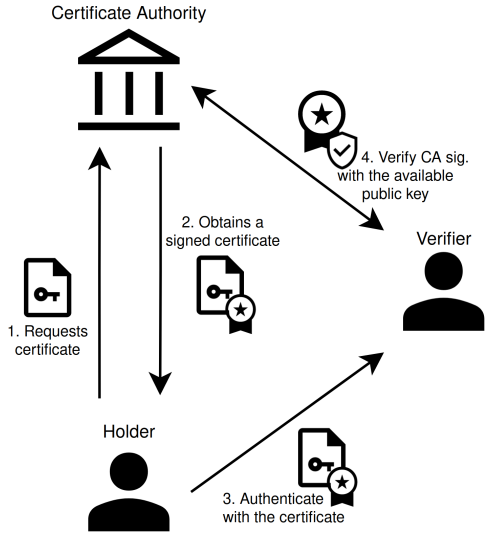
- Objectives:
  - Verify
  - Authenticate
    - Cannot be copied
  - Reduce phishing



https://infomaniak.com/en/certifications

State of the Art - Transport Layer Security (TLS)

- Based on Public Key Infrastructure (PKI)
- Uses X.509 certificates to bind web-servers to key pairs and domain names
- Provides encrypted connection



State of the Art - Transport Layer Security (TLS) - X.509

Domain Validated (DV) Certificate:

- Verifies that the applicant has control over the requested domain name
- Automatable: Automatic Certificate Management Environment (ACME)
- Can be free of charges when using ACME

Organisation Validated (OV) Certificate:

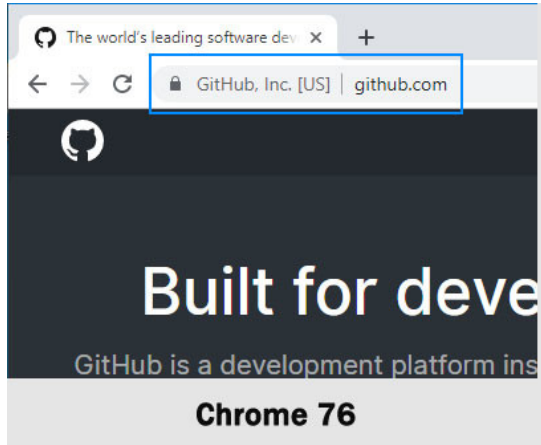
- DV verifications
- The legal existence and physical location of the applicant
- No automation possible
- Costs from 200 to +1000 USD per year

Extended Validation (EV) Certificate:

- OV verifications
- Legal status
- Operational existence
- Telephone verification
- No automation possible
- Costs from from 400 to +1700 USD per year

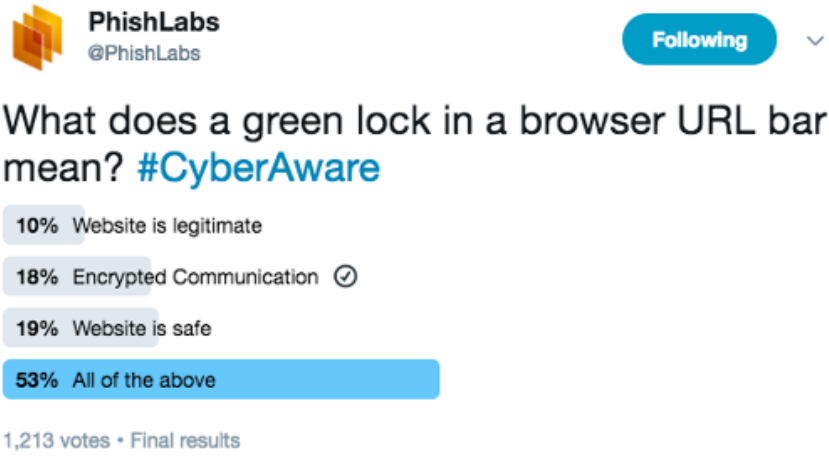
State of the Art - Transport Layer Security (TLS) - OV/EV Certificate

- Reduce fraud
- Green padlock
- Company name indicated
- Authenticity?



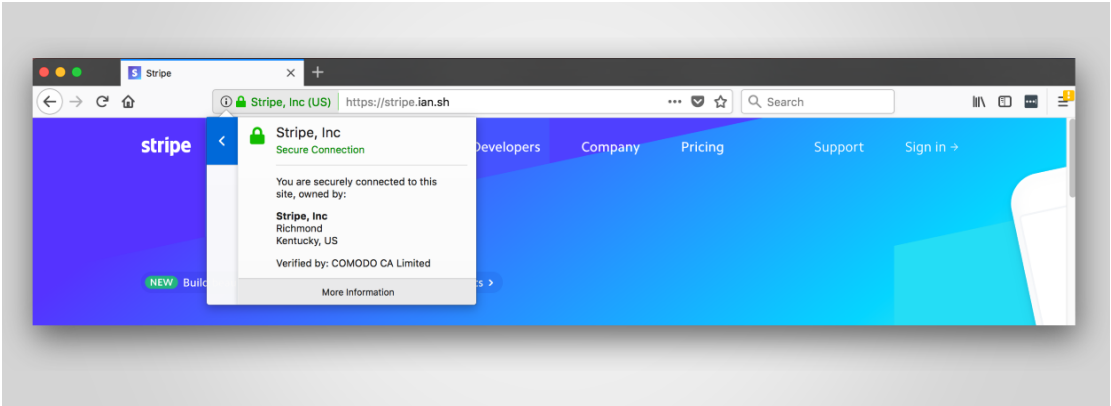
https://www.bleepingcomputer.com/news/software/chrome-and-firefox-changes-spark-the-end-of-ev-certificates

State of the Art - Transport Layer Security (TLS) - OV/EV Certificate



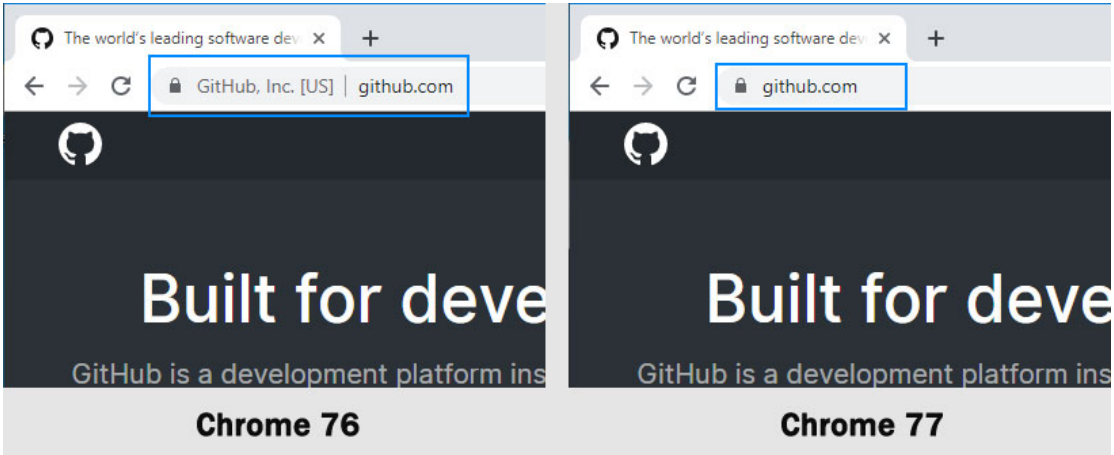
2017: https://www.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains

State of the Art - Transport Layer Security (TLS) - OV/EV Certificate



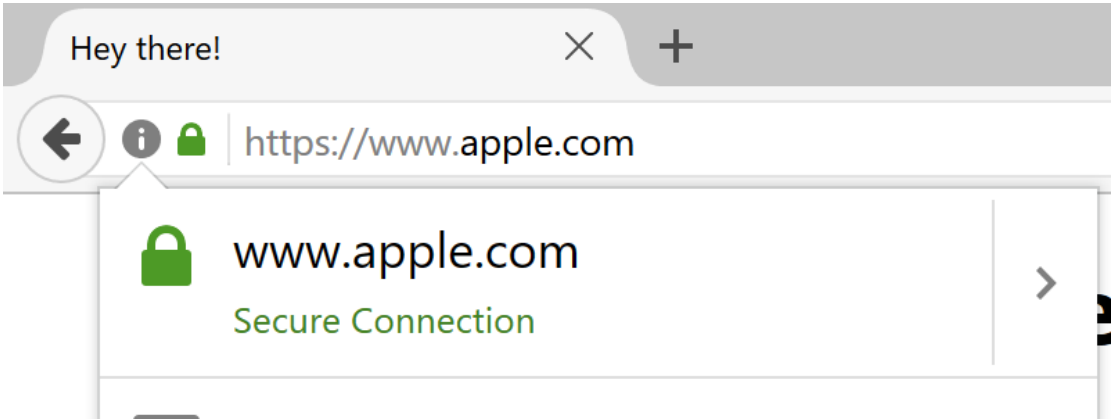
https://www.bleepingcomputer.com/news/security/extended-validation-ev-certificates-abused-to-create-insanely-believable-phishing-sites

State of the Art - Transport Layer Security (TLS) - OV/EV Certificate



https://www.bleepingcomputer.com/news/software/chrome-and-firefox-changes-spark-the-end-of-ev-certificates

State of the Art - Transport Layer Security (TLS) - OV/EV Certificate



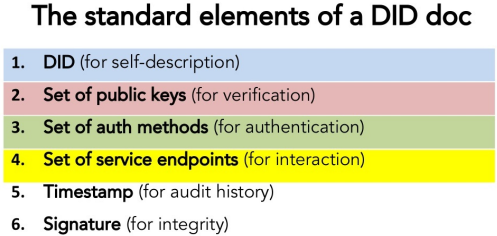
https://www.xudongz.com/blog/2017/idn-phishing/

State of the Art - Transport Layer Security (TLS) - OV/EV Certificate

- OVs / EVs are not sufficient for authenticity purposes:
  1. Misunderstood by the public
  2. Browsers removed the visual indicator
  3. Spoofing still possible (e.g. colliding entity name, unicode URLs)
  4. CAs are inconsistent
- That is why verifiable labels has to provide authentication.
- DVs issued with ACME are effective at binding domain names and key pair to a web-server

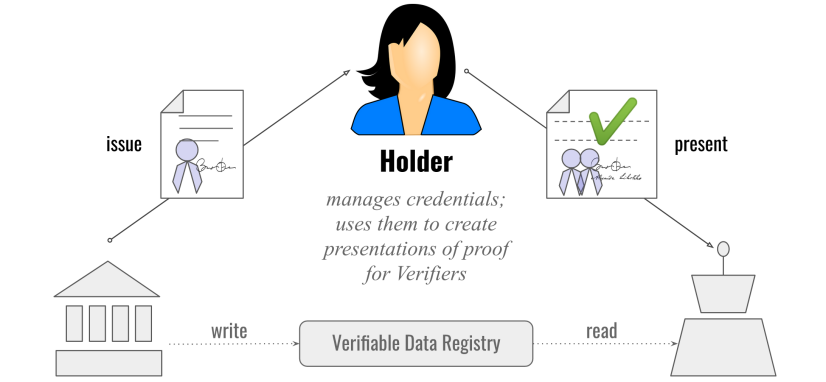
State of the Art - Decentralised Identifier (DID)

- Globally unique identifier
- Identify an entity
  - Verifiable
  - Permanent
  - Decentralised
- Resolves to a DID document



https://www.slideshare.net/SSIMeetup/
decentralized-identifiers-dids-the-fundamental-building-block-of-selfsovereign-ide

State of the Art - Decentralised Identifier (DID) - Verifiable Credential



https://commons.wikimedia.org/wiki/File:VC_triangle_of_Trust.svg

State of the Art - Decentralised Identifier (DID)

- Not everything is yet standardized:
  1. Linking an existing TLS certificate key pair to a DID
  2. VCs need a wallet with a functional, universal holder proof
- This solution is not yet defined and widely used enough to be applied in this specific use case
- DIDs leave an audit history with time stamps in the data registery

  → Reputation

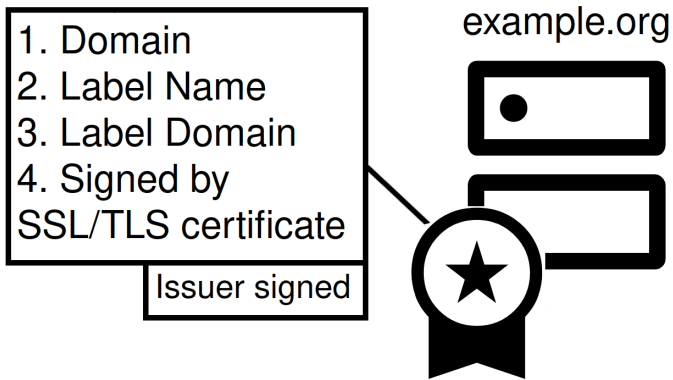
Concept - Trust

‘Trust is important, but it is also dangerous. It is important because it allows us to depend on others—for love, for advice, for help with our plumbing, or what have you—especially when we know that no outside force compels them to give us these things. But trust also involves the **risk** that people we trust will not pull through for us, for if there were some guarantee they would pull through, then we would have no need to trust them.
Trust is therefore **dangerous**. What we risk while trusting is the loss of valuable things that we entrust to others, …’

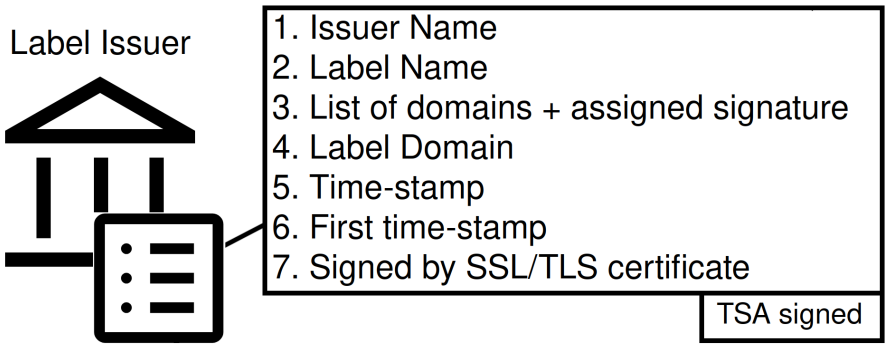
https://plato.stanford.edu/archives/fall2021/entries/trust

- Humans require facts to give their trust
- Cryptography creates tangible facts in the virtual world
- The system should strive to provide such facts instead of trying to distribute trust
- Users must be able to make the decision for themselves and not have to rely on a third-party organization they don’t even know exists

Concept - Definitions - Verifiable Label

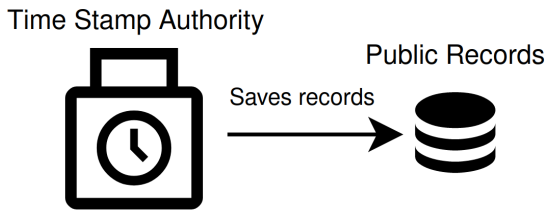


Concept - Definitions - Issuer

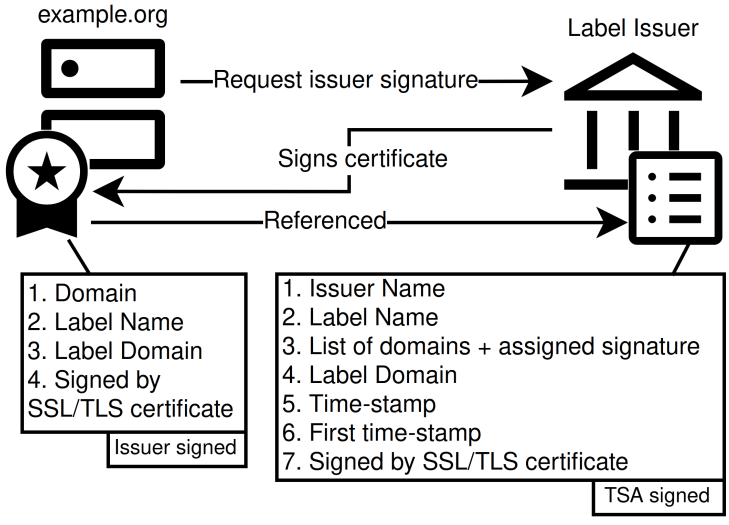


Concept - Definitions - Time Stamp Authority

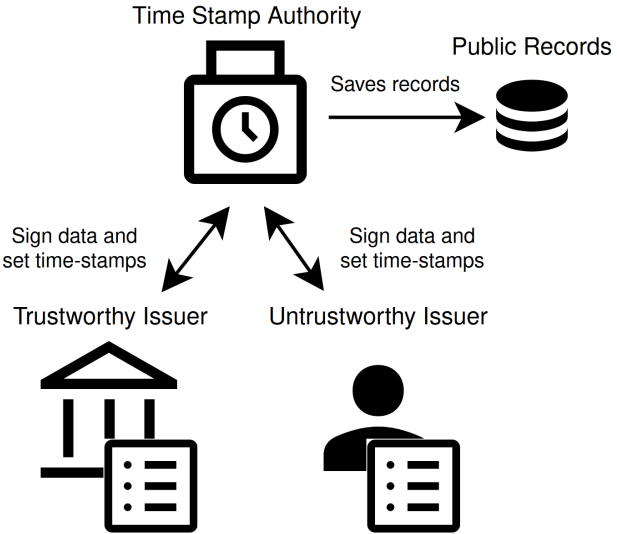
- Follows specific automated guidelines
- Every issuer plays by the same rules
- Guidelines aim at enforcing duplicate label prevention
- Reissuance is forced with the expiration of the issuer's certificate on a fixed time-period



Concept - Protocol - Issuance

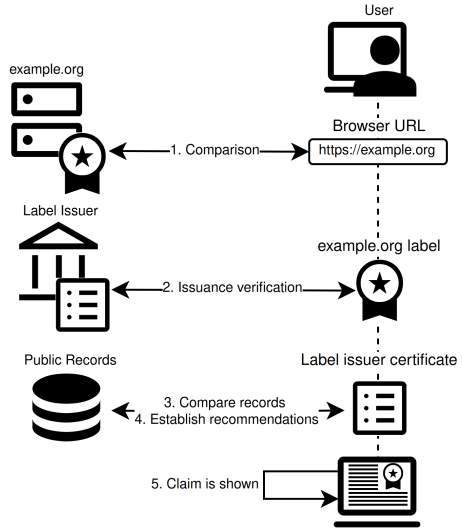


Concept - Protocol - Issuer Certification



Concept - Protocol - Validation and interpretation client

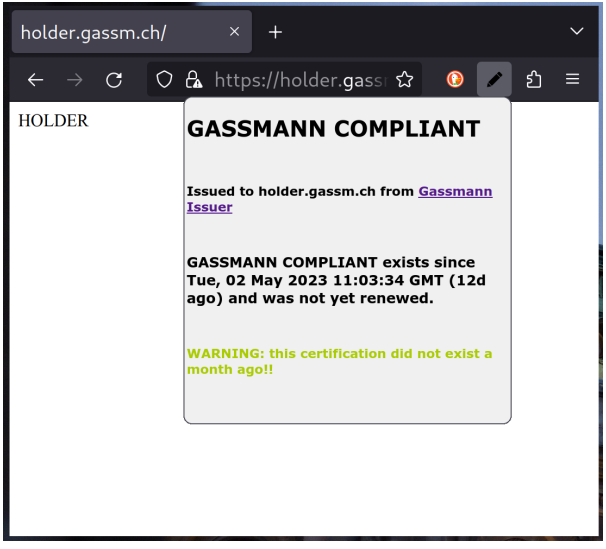
- Recommendation metrics are still to be defined, here are some examples:
  - Refreshment regularity
  - Time of existence
  - Measurement of the movement of certified entities
  - Activity ratio
  - Number of requests



Implementation

- Minimal working prototype
- Extensibility was a top priority
  - Verifiable Label Time Stamp Authority (VLTSA)
    - Is not a TSA; but a client
    - Still uses a TLS certificate to sign issuer's requests after the TSA signed it
    - HTTP POST /sign
    - HTTP GET /get_records
    - Abstract interfaces
  - Verifiable Label Issuer Client (VLIC)
    - Simple command-line client
    - Persistent storage
    - Takes arguments and save them
    - Can sign incomplete holder certificate and add it to its list
  - Verifiable Label Holder Client (VLHC)
    - Simple command-line client
    - No persistent storage
    - Simply generates an incomplete holder certificate from arguments
    - No channel specified
  - Browser Extension Analyzer
    - Needs to access current browser address
    - Browser extension environment was too limiting
    - Native messaging interface to communicate with underlying program

Implementation



Conclusion

- A solution was proposed:
  - To create verifiable labels
  - That strives to reduce fraud
- Reputation based system
- Rooted on TLS certificates and time stamp authorities but not limited to
- Simplistic but functional prototype

- Future work:
  - Conduct a field study of a live setup and user experience
  - Study relevant metadata for a good reputation evaluation
  - Provide a comprehensive UI for computers and phones

Questions

Questions ?