History of ID4me Protocol

- Single Sign On Solution (SSO)
- Alternative to Facebook and Google with enhanced privacy protection by design
- Chicken and Egg Conundrum
- Apple ID

Some Digital Identity Milestones

1988: X.509 distinguished name certificate system is launched

1992: "Web of Trust" concept first proposed for PGP certificates

1999: ICANN establishes current CPH WHOIS access framework

2005: First bi-annual meeting of the Internet Identity Workshop

2013: SIDN begins collaboration on the IRMA trust framework

2014: The European Parliament adopts the eIDAS regulation

2014: OpenID Foundation launches OpenID Connect

2015: The Australian DTA convenes work on a Digital Identity Framework

2016: LIGHTest begins testing a global cross-domain trust infrastructure

2017: W3C Verifiable Claims working Group is founded

2019: ID4Me announces a global standard for identity management

Unlikely Convergence of Events – Perfect Storm

- eIDAS – The EU regulation which established a set of standards for electronic identification and trust services for electronic transactions in the European Single Market

- UN's Sustainability Development Goals (SDGs) -

  Target 16.9: By 2030, provide legal identity for all, including birth registration

- US Treasury Report: A Financial System That Creates Economic Opportunities Nonbank Financials, Fintech, and Innovation

  Digital identity products and services hold promise for improving the trustworthiness, security, privacy, and convenience of identifying individuals and entities, thereby strengthening the processes critical to the movement of funds, goods, and data as the global economy races deeper into the digital age.

Value Proposition

- Use of the DNS as a trust anchor for digital identity resolution;
- Incorporating the use of validated federated Registrant credentials into the domain name eco-system;
- Increases potential business opportunities, increase business efficiency; and minimize potential legal liability.

Tales of Two Cities – Charles Dickens

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness ….

Worst of Times

- Industry growth slowing;
- Increased regulatory costs;
- Increased competition; and
- Potential increased liability

Worst of Times

A new **Digital Services Act** will upgrade our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market.

Digitalisation and cyber are two sides of the same coin. This starts with a different mindset: We need to move from "need to know" to "need to share".

We should do this through a **joint Cyber Unit** to speed up information sharing and better protect ourselves.

The public sector has an important role in stimulating digital transformation. I want the European Commission to lead by example.

I will drive the full digitalisation of the Commission, putting in place new digital methods and digital diplomacy tools.

Worst of Times

"Digital Services Act" I

Concept Note v7, 9 Ap

"b) **Outdated rules**
a variety of online
Name Registrars ar
they operate."

"d) **Ineffective pub**
Protection, Audio-
and Consumer Pro
regulator" in the E
in areas such as co

"The scope would
would address all s
ISPs to cloud hosti

"Digital Services Act" II

"The nature of such
update, clarify, and
Market, which could
into a Regulation.

"Updated scope.[...]
services, content de
media services, sear
online advertising se
contracts and distribu

"Intermediary liabil
general principle o
exemption continues
internet. The princip
to reflect the nature
application to [...]do

"Digital Services Act" III

"**Regulating content moderation**. Uniform rules for the removal of illegal content such as illegal hate speech would be made binding across the EU.[...]notice-and-action rules could be tailored to the types of services, e.g. whether the service is a social network, a mere conduit, or a collaborative economy service, and where necessary to the types of content in question[...]."

[...]"a clear distinction will be made between illegal and harmful content when it comes to exploring policy options.[...] in case of harmful content, codes of conduct and user empowerment in choosing sources could be given higher prominence; the role of the regulator could be strengthened (e.g. via approval of such codes of conduct)."

"**Regulatory oversight**.[...]Possible roles and powers of such regulatory structures will be explored, including reporting requirements, powers to require additional information, complaint handling, the power to impose fines or other corrective action, or the approval of codes of conduct[...]"

"**Cooperation with public authorities, including data access**.[...] a simpler interface with public authorities, including e.g. data access to public interest data sets."

5

Source: entr

Worst of Times

The EU Cybersecurity Act: a new Era dawns on ENISA

Today, 7th June 2019, the EU Cybersecurity Act was published in the Official Journal of the European Union.

(23) The public core of the open internet, namely its main protocols and infrastructure, which are a global public good, provides the essential functionality of the internet as a whole and underpins its normal operation. ENISA should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS, BGP, and IPv6), **the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone**.

Worst of Times

NTIA Statement on Amendment 35 to the Cooperative Agreement with Verisign

Topics: **Domain Name System**

Printer-friendly version

FOR IMMEDIATE RELEASE:

November 01, 2018

News Media Contact:

Anne Veigle, (202) 482-4208, **aveigle@ntia.gov**

NTIA and Verisign have agreed to extend and modify the **Cooperative Agreement**. These modifications are in line with policy priorities of the Trump Administration. The changes create a new commitment to content neutrality in the Domain Name System (DNS), provide market-based pricing flexibility, and reduce the regulatory burden on Verisign.

Amendment 35 confirms that Verisign will operate the .com registry in a content neutral manner with a commitment to participate in ICANN processes. To that end, NTIA looks forward to working with Verisign and other ICANN stakeholders in the coming year on trusted notifier programs to provide transparency and accountability in the .com top level domain.

The amendment repeals Obama-era price controls and provides Verisign the pricing flexibility to change its *.com* Registry Agreement with ICANN to increase wholesale .com prices. Specifically, the flexibility permits Verisign to pursue with ICANN an up to 7 percent increase in the prices for .com domain names, in each of the last four years of the six-year term of the .com Registry Agreement. The changes also affirm that Verisign may not vertically integrate or operate as a registrar in the .com top level domain.

Worst of Times

ICANN | GAC

Governmental Advisory Committee

Distribution	Public
Date	18 September 2019

GAC Statement on DNS Abuse

ICANN's Governmental Advisory Committee (GAC) looks forward to the upcoming cross-community discussion on DNS Abuse during ICANN66 and appreciates the Registries Stakeholder Group's August 19, 2019 Open Letter to the Community on this topic.

Protecting the public from security threats and DNS Abuse is an important public policy issue. The GAC has issued advice, provided guidance and comments, organized cross-community discussions, and advocated for stronger contractual provisions to safeguard the public.[1] Our current remarks will provide further context on this topic by discussing: 1) why DNS Abuse is a vital topic; 2) the existing definitions and contractual obligations regarding DNS Abuse; and 3) the Competition, Consumer Trust, and Consumer Choice Review Team's findings and recommendations on DNS Abuse. Through this discussion, we hope to lay the foundation for a productive and informed cross-community discussion in Montreal.

Best of Times

- Several ccTLD are taking a thought leadership role and being recognized for it

GAC Statement on DNS Abuse

ccTLD Registries' Best Practices

In recent years, an increasing number of ccTLD registries have adopted pro-active anti-abuse measures to address DNS-facilitated crime and both keep their zone free of abuse and repel bad actors by making their domain names as unattractive to bad actors as possible. These measures range from stronger authentication methods, including identity checks,[24] to the use of data-based fraud prediction models which combine data registration and infrastructure metrics to identify and predict domain registrations made for harmful purposes.[25] These proven best practices should be implemented by gTLD registries and registrars.

---

[23] CCT Final Report at p. 94, citing DNS Abuse Study at pp. 24-25.

[24] See e.g., ICANN64 Session on Lessons Learned: How .DK successfully reduced abusive domains and https://www.dk-hostmaster.dk/en/news/mandatory-identification-nemid and https://www.dk-hostmaster.dk/en/news/dk-hostmaster-makes-online-fraud-more-difficult

[25] See https://eurid.eu/en/news/identification-of-malicious-dns/

GAC Statement on DNS Abuse – 18 September 2019 – Page 4

Best of Times

- eIDAS Regulation (EU) No 910/2014
- Mandatory recognition of eID (09.2018)
- Mandatory recognition of “electronic identification means”
  a material and/or immaterial unit containing person identification data and which is used for authentication for an online service. (ID-cards, Mobile-ID’s, Smart-ID, etc.)
- Must recognize ‘notified’ eIDs of other Member States for cross-border access to its online services when its national laws mandate e-identification

Best of Times

- Several ccTLDs in collaboration with CENTR have engaged in potential solutions regarding identity.

EUROPEAN COMMISSION
Innovation and Networks Executive Agency

Connecting Europe Facility 2014-2020

CEF TELECOM CALL FOR PROPOSALS 2018
CEF-TC-2019-1

Title of the proposed Action RegeID

TENtec number 28631003

The project in line with the call "CEF-TC-2019-1: eIdentification (eID) & eSignature", focuses on the integration of eID DSI (Digital Service Infrastructures) in e-services and administrator systems of national domains of the Czech Republic (.CZ), Denmark (.DK), Estonia (.EE) and The Netherlands (.NL). Although the relevant domain names (ccTLDs) are managed by private-law entities, these services report elements of public services, as evidenced by the fact that all three project partners have a Memorandum or agreement with the relevant government bodies on the operation and management of the relevant ccTLDs.

This action will open up registrant-services from 4 national top level domain registries to the eIDAS-infrastructure and as thus to the citizens of all European countries.

These services are relevant to registrants of domain names (both individuals and organisations). Encompassing 8.5 million domain names in total, it will allow registrants to secure their information on these domain names through their national eIDs and enhance trust, assurance and security in the entire internet environment.

The importance of the project for cross-border cooperation and Digital Single Market can be demonstrated on the following number of domain holders from another country:

- .CZ: 1.3 million domain names (75.000 registered to other EU citizens)
- .DK: 1.3 million domain names (36.000 registered to other EU citizens/entities)
- .EE: 121.000 domain names (12.000 registered to other EU citizens/entities)
- .NL: 5.8 million domain names (250.000+ registered to other EU citizens/entities)

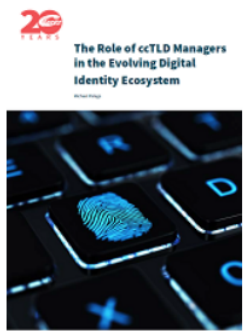
Best of Times

- Many other ccTLDs are taking proactive steps to integrate digital identity into their domain name registration business flow:

Library

Library **Legal case library**

20th Anniversary Paper: The Role of ccTLD Managers in the Evolving Digital Identity Ecosystem



Date: 2019-02-13
Category: Educational /promotional material
Additional filters: Michael Palage

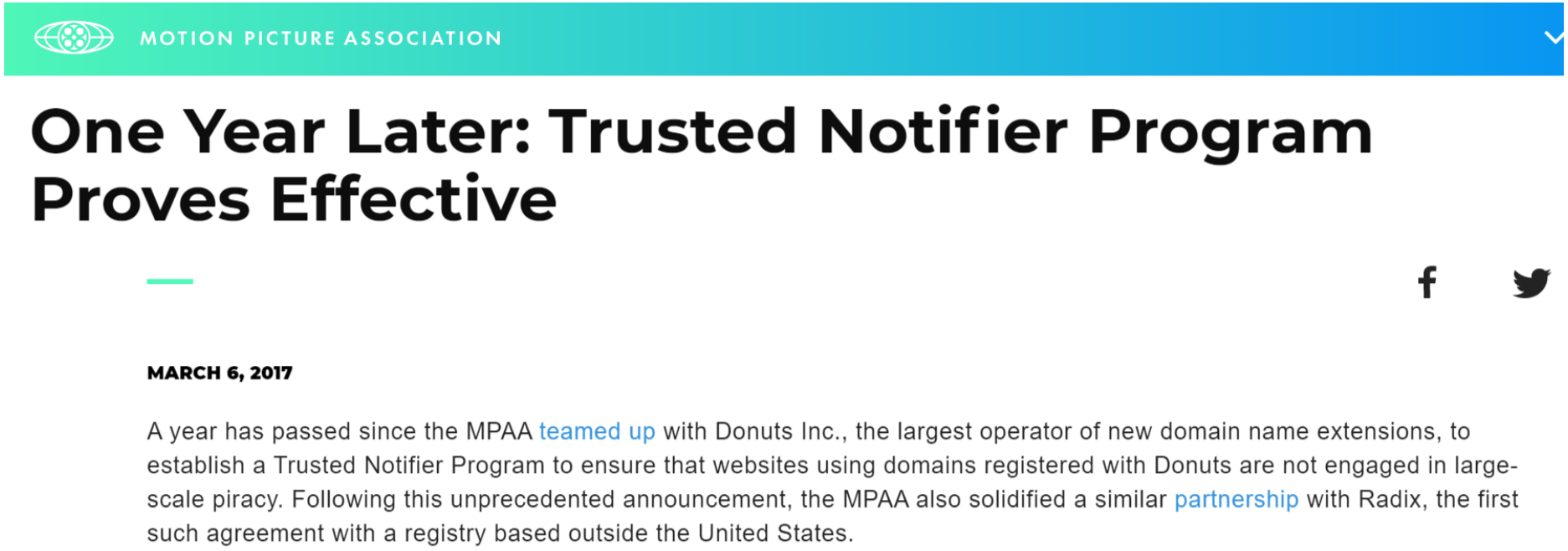
← BACK DOWNLOAD →

Example: ICANN's Unified Access Model

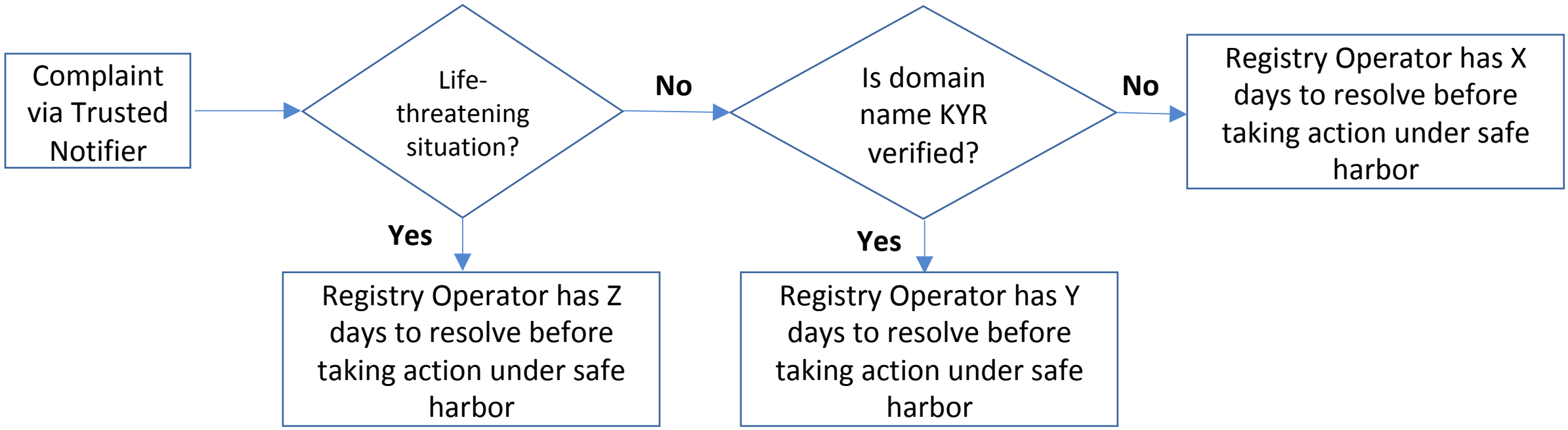
- Know Your Registrant (KYR)
- Similarities/Differences between Know Your Registrant (KYR) and Know Your Customer (KYC)
- Potential key component in ICANN's Unified Access Model (UAM)

Example: Trusted Notifier

- Trusted Notifiers play a key role in the ability of any Registration Authority (Registry or Registrar) to implement any Notice and Take Down framework.



Example: Trusted Notifier



Rules of Engagement: Z < Y < X, where Z is the response time associated with an imminent life-threatening situation, Y is the response time for non- imminent life-threatening situation of a known registrant (KYR), and X is the response time for non-imminent life-threatening situation of a un-known registrant (KYR)

Call to Action

- Potential collaboration on an agreed upon EPP extension (potential RFC) to handle identity in the domain name registration process;
- Increased educational outreach and education on all-things “identity” related, and the need for a clearinghouse / repository

Thank You