Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

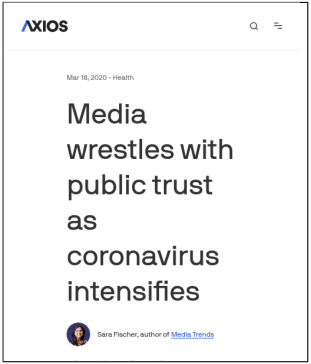
Pouyan Fotouhi Tehrani[1], Eric Osterweil[2], Jochen Schiller[3], Thomas C. Schmidt[4], Matthias Wählisch[3]

[1]Weizenbaum Institut / Fraunhofer FOKUS [2]George Mason University [3]Freie Universität Berlin [4]Hamburg University of Applied Sciences

30th The Web Conference, April 19-23, 2021.

Alerting Authorities are crucial during crises.

- People rely on **trustworthy sources**.



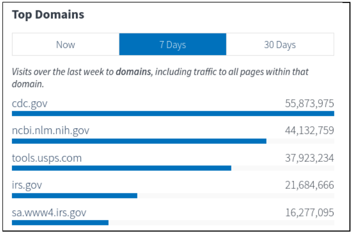
Mar 18, 2020 - Health

Media wrestles with public trust as coronavirus intensifies

Sara Fischer, author of Media Trends

Alerting Authorities are crucial during crises.

- People rely on **trustworthy sources**.
- Authorities provide services **via web**.



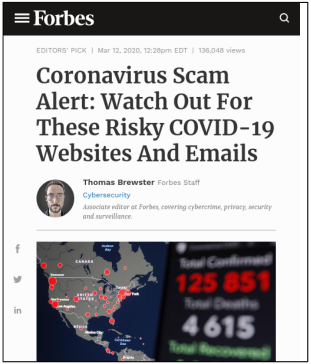
Top Domains

*Visits over the last week to **domains**, including traffic to all pages within that domain.*

cdc.gov	55,873,975
ncbi.nlm.nih.gov	44,132,759
tools.usps.com	37,923,234
irs.gov	21,684,666
sa.www4.irs.gov	16,277,095

Alerting Authorities are crucial during crises.

- People rely on **trustworthy sources**.
- Authorities provide services **via web**.
- Evaluating **trustworthiness** is a challenge.



Forbes

EDITORS' PICK | Mar 12, 2020, 12:28pm EDT | 136,048 views

Coronavirus Scam Alert: Watch Out For These Risky COVID-19 Websites And Emails

Thomas Brewster Forbes Staff

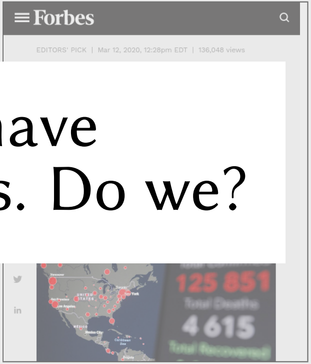
Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Alerting Authorities are crucial during crises.

- Pe
- Au
- Ev

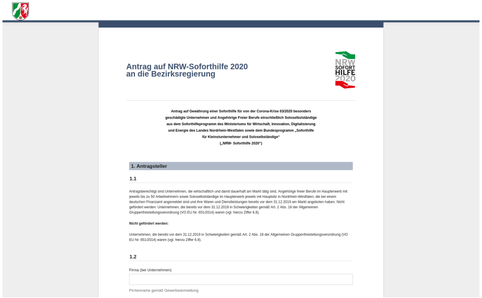
But wait, we do have protection mechanisms. Do we?



Forbes

EDITORS' PICK | Mar 12, 2020, 12:28pm EDT | 136,048 views

Scammers Attack a German Paycheck Protection Plan. True Story.



NRW SOFORT HILFE 2020

Antrag auf NRW-Soforthilfe 2020
an die Bezirksregierung

Antrag auf Gewährung einer Soforthilfe für von der Corona-Krise 03/2020 besonders
geschädigte Unternehmen und Angehörige Freier Berufe einschließlich Soloselbstständige
aus dem Soforthilfeprogramm des Ministeriums für Wirtschaft, Innovation, Digitalisierung
und Energie des Landes Nordrhein-Westfalen sowie dem Bundesprogramm „Soforthilfe
für Kleinstunternehmer und Soloselbständige"
(„NRW- Soforthilfe 2020")

1. Antragsteller

1.1

Antragsberechtigt sind Unternehmen, die wirtschaftlich und damit dauerhaft am Markt tätig sind, Angehörige freier Berufe im Haupterwerb mit jeweils bis zu 50 Arbeitnehmern sowie Soloselbstständige im Haupterwerb jeweils mit Hauptsitz in Nordrhein-Westfalen, die bei einem deutschen Finanzamt angemeldet sind und ihre Waren und Dienstleistungen bereits vor dem 31.12.2019 am Markt angeboten haben. Nicht gefördert werden: Unternehmen, die bereits vor dem 31.12.2019 in Schwierigkeiten gemäß Art. 2 Abs. 18 der Allgemeinen Gruppenfreistellungsverordnung (VO EU Nr. 651/2014) waren (vgl. hierzu Ziffer 6.8).

Nicht gefördert werden:

Unternehmen, die bereits vor dem 31.12.2019 in Schwierigkeiten gemäß Art. 2 Abs. 18 der Allgemeinen Gruppenfreistellungsverordnung (VO EU Nr. 651/2014) waren (vgl. hierzu Ziffer 6.8).

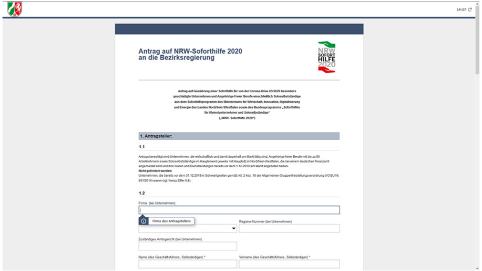
1.2

Firma (bei Unternehmen)

Firmenname gemäß Gewerbeanmeldung

`https://nrw-corona-soforthilfe.de`

?



14:57

NRW SOFORT HILFE 2020

Antrag auf NRW-Soforthilfe 2020
an die Bezirksregierung

Antrag auf Gewährung einer Soforthilfe für von der Corona-Krise 03/2020 besonders
geschädigte Unternehmen und Angehörige Freier Berufe einschließlich Soloselbstständige
aus dem Soforthilfeprogramm des Ministeriums für Wirtschaft, Innovation, Digitalisierung
und Energie des Landes Nordrhein-Westfalen sowie des Bundesprogramms „Soforthilfen
für Kleinstunternehmer und Soloselbständige"
(„NRW- Soforthilfe 2020")

1. Antragsteller:

1.1

Antragsberechtigt sind Unternehmen, die wirtschaftlich und damit dauerhaft am Markt tätig sind, Angehörige freier Berufe mit bis zu 50 Arbeitnehmern sowie Soloselbstständige im Haupterwerb jeweils mit Hauptsitz in Nordrhein-Westfalen, die bei einem deutschen Finanzamt angemeldet sind und ihre Waren und Dienstleistungen bereits vor dem 1.12.2019 am Markt angeboten haben.
Nicht gefördert werden:
Unternehmen, die bereits vor dem 31.12.2019 in Schwierigkeiten gemäß Art. 2 Abs. 18 der Allgemeinen Gruppenfreistellungsverordnung (VO EU Nr. 651/2014) waren (vgl. hierzu Ziffer 6.8).

1.2

Firma (bei Unternehmen)

Firma des Antragstellers

Register-Nummer (bei Unternehmen)

Zuständiges Amtsgericht (bei Unternehmen)

Name (des Geschäftsführers, Selbständigen) *

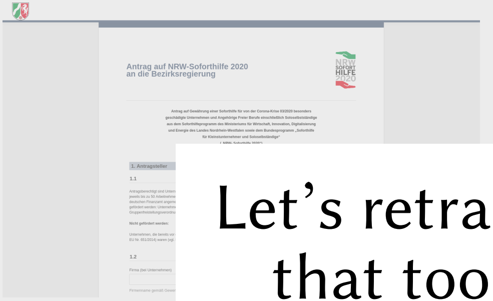
Vorname (des Geschäftsführers, Selbständigen) *

`https://soforthilfe-corona.nrw.de`

- ✓ Sound domain name under `.de`
- ✓ HTTPS enabled
- ✓ DNSSEC enabled

- ✓ Sound domain name under `.de`
- ✓ HTTPS enabled
- ✗ DNSSEC not enabled

Scammers Attack a German Paycheck Protection Plan. True Story.



Antrag auf NRW-Soforthilfe 2020
an die Bezirksregierung

Antrag auf Gewährung einer Soforthilfe für von der Corona-Krise 03/2020 besonders geschädigte Unternehmen und Angehörige Freier Berufe einschließlich Soloselbstständige aus dem Soforthilfeprogramm des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen sowie dem Bundesprogramm „Soforthilfe für Kleinstunternehmer und Soloselbständige"
(„NRW- Soforthilfe 2020")

1. Antragsteller

1.1

Antragsberechtigt sind Untern
jeweils bis zu 50 Arbeitnehme
deutschen Finanzamt angeme
gefördert werden: Unternehme
Gruppenfreistellungsverordnu

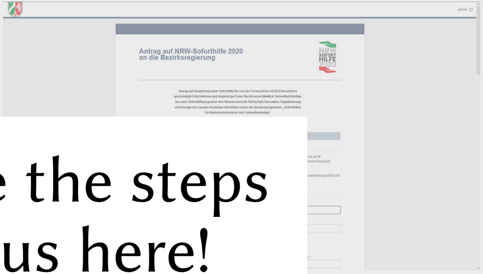
Nicht gefördert werden:

Unternehmen, die bereits vor
EU Nr. 651/2014) waren (vgl.

1.2

Firma (bei Unternehmen)

Firmenname gemäß Gewer



Antrag auf NRW-Soforthilfe 2020
an die Bezirksregierung

Antrag auf Gewährung einer Soforthilfe für von der Corona-Krise 03/2020 besonders geschädigte Unternehmen und Angehörige Freier Berufe einschließlich Soloselbstständige aus dem Soforthilfeprogramm des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen sowie des Bundesprogramms „Soforthilfen für Kleinstunternehmer und Soloselbständige"

bis zu 50
chen Finanzamt
sverordnung (VO EU Nr.

https://nrw-

orona.nrw.de

Let's retrace the steps
that took us here!

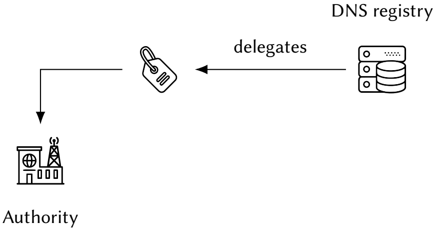
- ✓ Sound domain name under .de
- ✓ HTTPS enabled
- ✓ DNSSEC enabled

- ✓ Sound domain name under .de
- ✓ HTTPS enabled
- ✗ DNSSEC not enabled

Secure Web-based Communication. A Complex System.

Authority

Secure Web-based Communication. A Complex System.

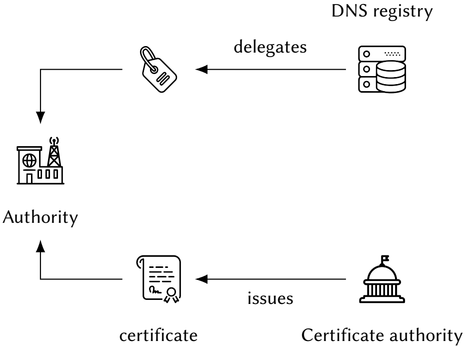


DNS registry

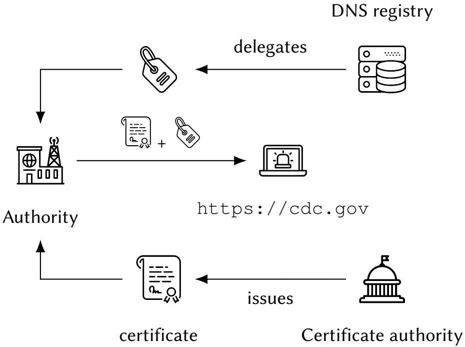
delegates

Authority

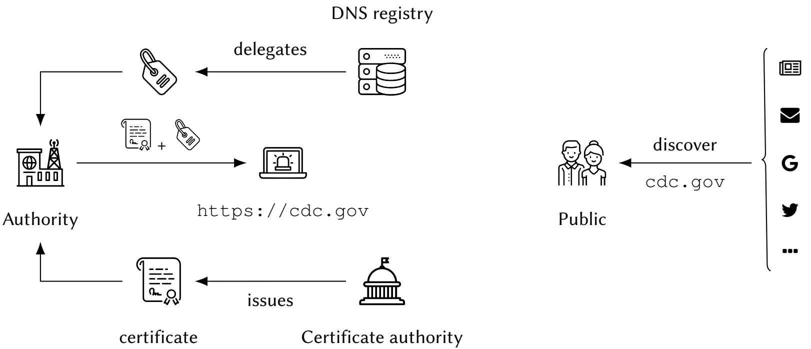
Secure Web-based Communication. A Complex System.



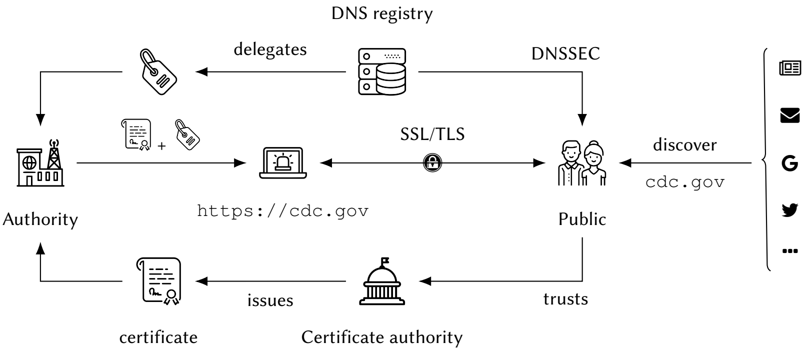
Secure Web-based Communication. A Complex System.



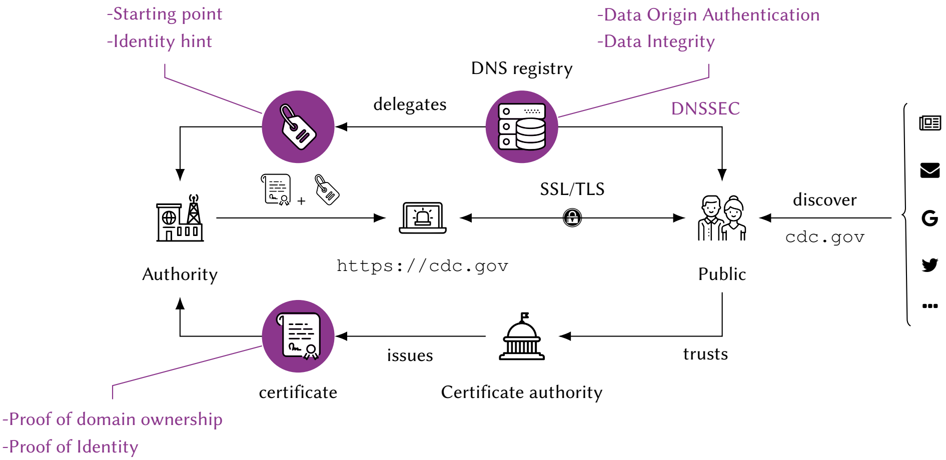
Secure Web-based Communication. A Complex System.



Secure Web-based Communication. A Complex System.



Secure Web-based Communication. A Complex System.



Secure Web-based Communication. A Complex System.

-Starting point
-Identity hint

-Data Origin Authentication
-Data Integrity

DNS registry

We contribute:

(1) A threat model for Web-based communication.

(2) A method to discover and analyze Alerting Authorites.

(3) Web security profiles of Alerting Authorities in the US.

certificate

Certificate authority

-Proof of domain ownership
-Proof of Identity

Threat Model. Three Dimensions.

Identification Securely authenticating the person, etc. behind the service name.

Threat Model. Three Dimensions.

Identification Securely authenticating the person, etc. behind the service name.

Resolution Securely verifying that users have not been misdirected and are transacting with the service name they have identified.

Threat Model. Three Dimensions.

Identification Securely authenticating the person, etc. behind the service name.

Resolution Securely verifying that users have not been misdirected and are transacting with the service name they have identified.

Transaction Ensuring that the content was not altered, leaks privacy etc. during the session.

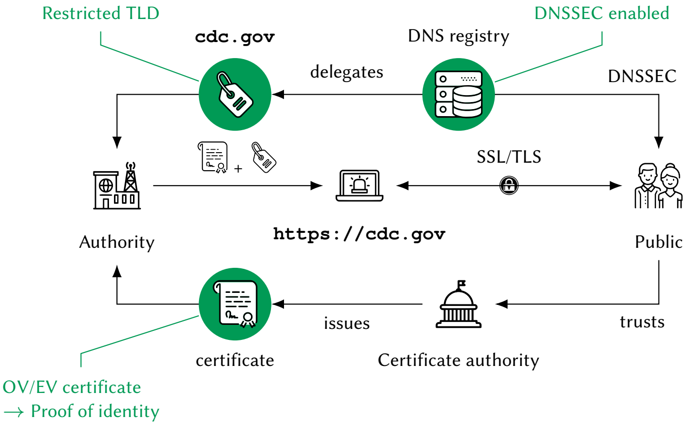
Threat Model. Three Dimensions.

Identification Securely authenticating the person, etc. behind the service name.

How DNS(SEC) and WebPKI amount to secure communicaiton?

the session.

Secure Web-based Communication. Assurance Profiles.



Restricted TLD

`cdc.gov`

DNS registry

DNSSEC enabled

delegates

DNSSEC

+

SSL/TLS

Authority

`https://cdc.gov`

Public

issues

trusts

certificate

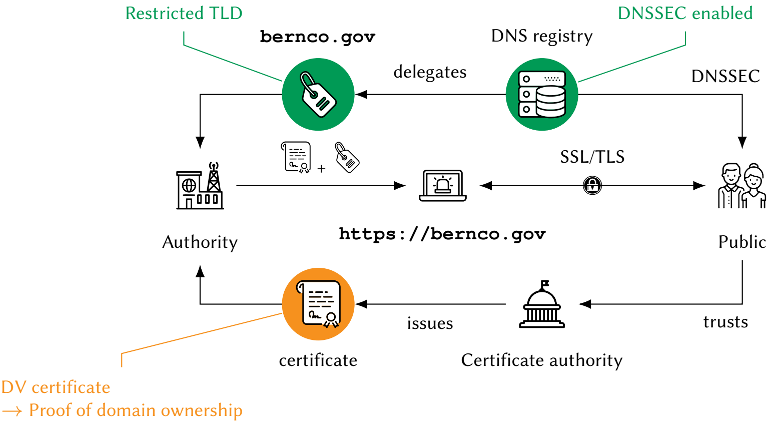
Certificate authority

OV/EV certificate
→ Proof of identity

● Strong Assurance:

- 👍 Identification
- 👍 Resolution
- 👍 Transaction

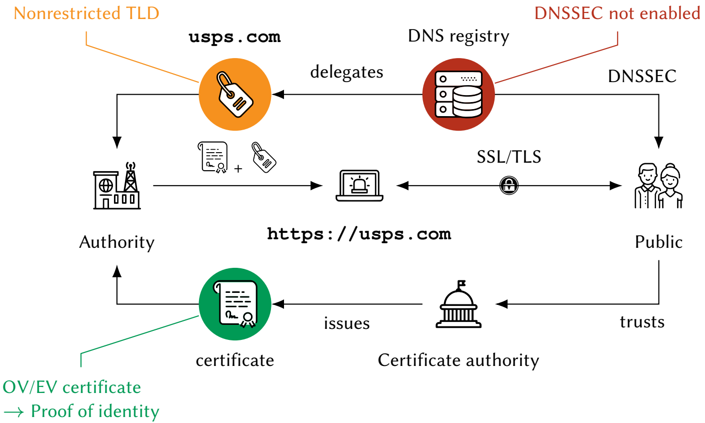
Secure Web-based Communication. Assurance Profiles.



◐ Weak Assurance:

- ⚠ Identification
- 👍 Resolution
- 👍 Transaction

Secure Web-based Communication. Assurance Profiles.



Nonrestricted TLD

usps.com

DNS registry

DNSSEC not enabled

delegates

DNSSEC

SSL/TLS

Authority

https://usps.com

Public

issues

trusts

certificate

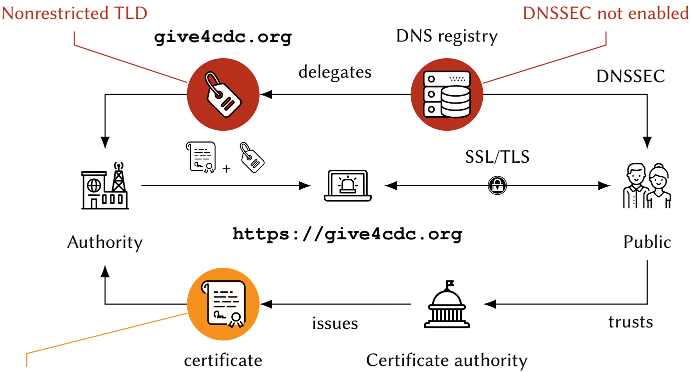
Certificate authority

OV/EV certificate
→ Proof of identity

◐ Weak Assurance:

- ⚠ Identification
- 👎 Resolution
- 👍 Transaction

Secure Web-based Communication. Assurance Profiles.



DV certificate
⟶ Proof of domain ownership

○ Inadequate Assurance:

- 👎 Identification
- 👎 Resolution
- 👍 Transaction

Threat Model in context. Assurance profiles.

	DNS		Web PKI		Security Implications				Assurance Profile
#	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction	Weakness	
01	✓	✓	–	✓	👍	👍	👍	N/A	●
02	✓	✓	✓	✗	⚠	👍	👍	Ambiguous identification	◐
03	✗	✓	–	✓	⚠	👍	👍	Possible impersonation through name spoofing	◐
04	✓	✗	–	✓	⚠	👎	👍	DNS hijacking	◐
05	✗	✗	–	✓	⚠	👎	👍	Name spoofing, DNS hijacking	◐
06	✓	✗	✓	✗	⚠	👎	👍	DNS hijacking and ambiguous identification	○
07	✗	✗	✓	✗	👎	👎	👍	Impersonation and DNS hijacking	○
08	✗	✓	✓	✗	👎	👍	👍	Impersonation	○
09	✓	✓	✗	✗	👎	👎	👎	Content poisoning	○
10	✓	✗	✗	✗	👎	👎	👎	DNS hijacking, content poisoning	○
11	✗	✓	✗	✗	👎	👍	👎	Impersonation, content poisoning	○
12	✗	✗	✗	✗	👎	👎	👎	DNS hijacking, impersonation, content poisoning	○

Threat Model in context. Assurance profiles.

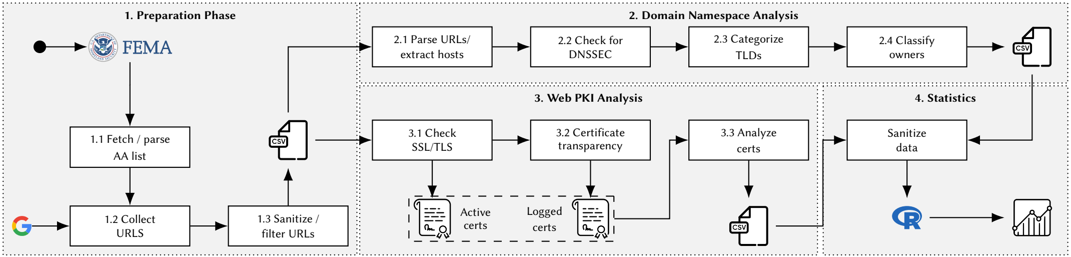
	DNS		Web PKI		Security Implications				
#	Restricted TLD	DNSSEC	DV	OV/EV	Identification	Resolution	Transaction	Weakness	Assurance Profile
01	✓	✓	–	✓	👍	👍	👍	N/A	●
02	✓	✓	✓	✗	⚠	👍	👍	Ambiguous identification	◐
03	✗	✓	–	✓	⚠	👍	👍	Possible impersonation through name spoofing	◐
04	✓	✗	–	[illegible]	[illegible]	[illegible]	👍	DNS hijacking	◐
05	✗	✗	–	[illegible]	[illegible]	[illegible]	👍	Name spoofing, DNS hijacking	◐
06	✓	✗	✓	[illegible]	[illegible]	[illegible]	👍	DNS hijacking and ambiguous identification	○
07	✗	✗	✓	✗	👎	👎	👍	Impersonation and DNS hijacking	○
08	✗	✓	✓	✗	👎	👍	👍	Impersonation	○
09	✓	✓	✗	✗	👎	👎	👎	Content poisoning	○
10	✓	✗	✗	✗	👎	👎	👎	DNS hijacking, content poisoning	○
11	✗	✓	✗	✗	👎	👍	👎	Impersonation, content poisoning	○
12	✗	✗	✗	✗	👎	👎	👎	DNS hijacking, impersonation, content poisoning	○

Details see paper.

Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

Methodology, Toolchain, and Data Set

Measurement Period October 2019 – March 2020



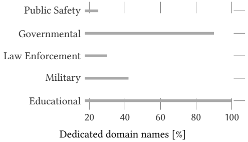
1388 Alerting Authorities in the US → 1365 URLs → 1327 unique hosts

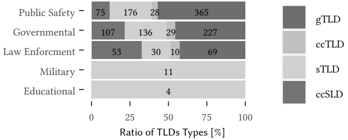
Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

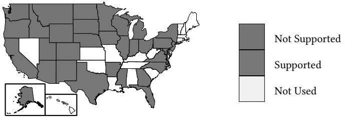
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- **Does each AA have its own dedicated domain name?**
- **How do AAs integrate in the global DNS namespace?**
- **Do AAs secure their names using DNSSEC?**





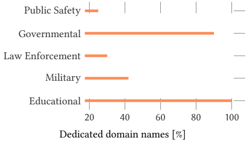


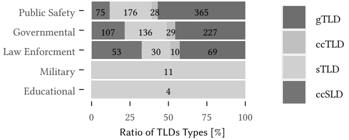
DNSSEC for `<state>.us`

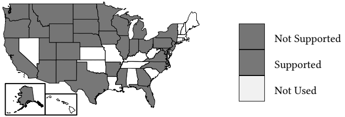
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- **Does each AA have its own dedicated domain name?**
  About 49% of Alerting Authorities do not have dedicated names,
  e.g., `https://www.vercounty.org/ema.htm`
  → unnecessary dependencies, *e.g.*, for X.509 certificates.





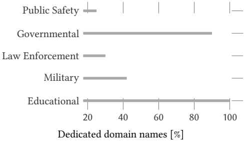


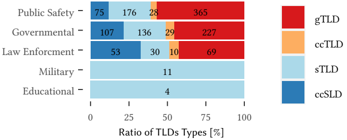
DNSSEC for `<state>.us`

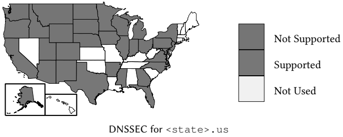
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- About 49% of Alerting Authorities do not have dedicated names
- **How do AAs integrate in the global DNS namespace?**
  More than 50% of unique names are under **non**-restricted TLDs
  → poor recognizability and inferior security.



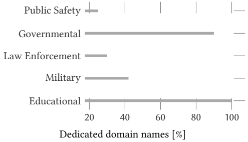


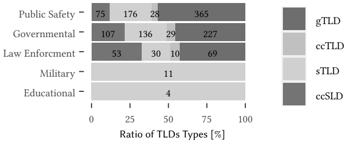


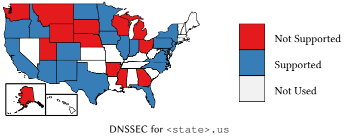
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- About 49% of Alerting Authorities do not have dedicated names
- More than 50% of unique names are under **non**-restricted TLDs
- **Do AAs secure their names using DNSSEC?**
  96% of unique hosts do not support DNSSEC
  → high susceptibility to DNS hijacking



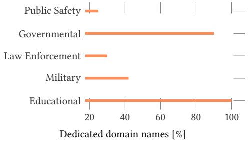


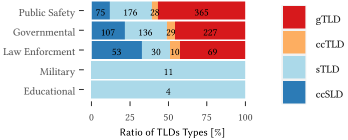


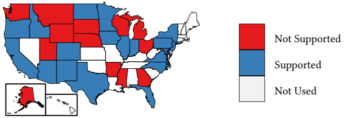
Results: Namespace and DNS(SEC) Analysis

1327 Unique Hosts

- About 49% of Alerting Authorities do not have dedicated names
- More than 50% of unique names are under **non**-restricted TLDs
- 96% of unique hosts do not support DNSSEC







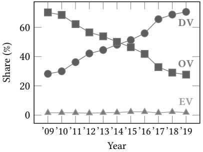
DNSSEC for `<state>.us`

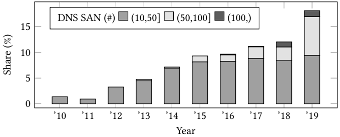
Security of Alerting Authorities in the WWW: Measuring Namespaces, DNSSEC, and Web PKI

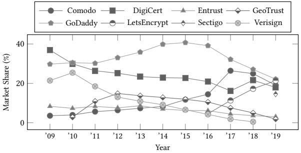
Results: Web PKI Analysis

1327 Unique Hosts

- **To what extent do AAs adapt web PKI?**
- **How is the historic landscape of X.509 shaped among AAs?**



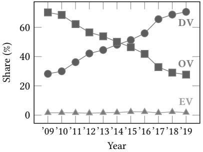


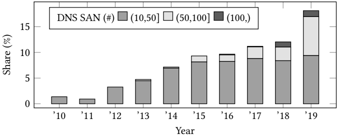


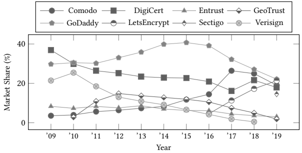
Results: Web PKI Analysis

1327 Unique Hosts

- **To what extent do AAs adapt web PKI?**
  About 15% provide none or invalid certificates
  → secure identification and transaction impossible



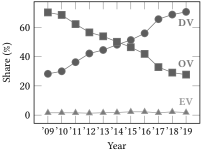


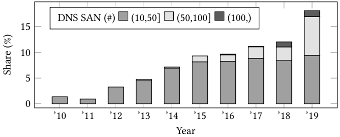


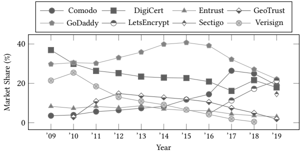
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 shaped among AAs?**



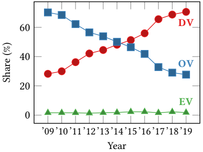


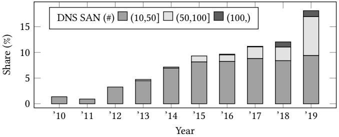


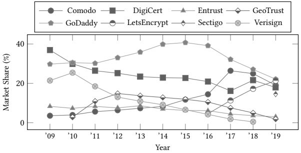
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 shaped among AAs?**
  - **Which validation types have been popular?**
    OV/EV certificates are losing popularity







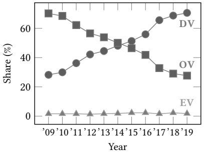
Results: Web PKI Analysis

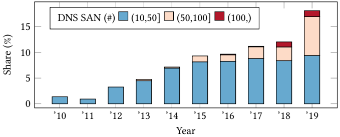
1327 Unique Hosts

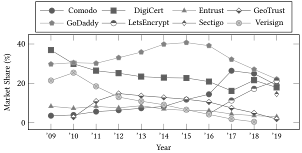
- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 shaped among AAs?**
  - OV/EV certificates are losing popularity
  - **Has certificate usage been exclusive?**

    Certificate sharing is on the rise

    → fate-sharing is increasing







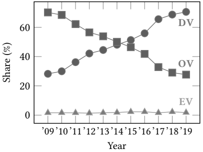
Results: Web PKI Analysis

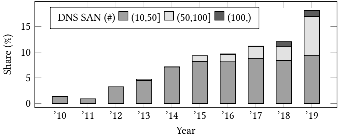
1327 Unique Hosts

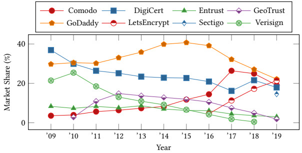
- About 15% provide none or invalid certificates
- **How is the historic landscape of X.509 shaped among AAs?**
  - OV/EV certificates are losing popularity
  - Certificate sharing is on the rise
  - **How has the CA market been changed?**

    CA giants are losing to free and automated DV certificate issuers

    → AAs care more about encryption than identification



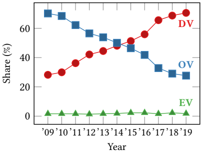


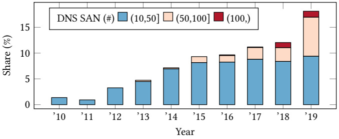


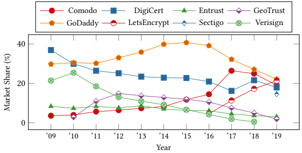
Results: Web PKI Analysis

1327 Unique Hosts

- About 15% provide none or invalid certificates
- OV/EV certificates are losing popularity
- Certificate sharing is on the rise
- CA giants are losing to free and automated DV certificate issuers







Security of Alerting Authorities in the WWW:

Measuring Namespaces, DNSSEC, and Web PKI

Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	126
				Total:	1036 (≈ 78%)
				Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.
- About 67% provide inadequate assurance because of vulnerable identification and resolution.

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	126
				Total:	1036 (≈ 78%)
				Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.
- About 67% provide inadequate assurance because of vulnerable identification and resolution.
- About 15% of all fail to provide valid certificates (inadequate assurance profile).

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✘	◐	11
✘	✓	–	✓	◐	2
✓	✘	–	✓	◐	132
✘	✘	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✘	✓	✘	○	354
✘	✘	✓	✘	○	482
✘	✓	✓	✘	○	3
✓	✓	✘	✘	○	2
✓	✘	✘	✘	○	67
✘	✓	✘	✘	○	2
✘	✘	✘	✘	○	126
				Total:	1036 (≈ 78%)
				Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

Putting the Pieces Together

- Only about 22% exhibit strong or weak assurance profiles.
- About 67% provide inadequate assurance because of vulnerable identification and resolution.
- About 15% of all fail to provide valid certificates (inadequate assurance profile).

DNS		Certificate			
Restricted delegation	Supports DNSSEC	DV	O/EV	Assurance profile[1]	# Names
✓	✓	–	✓	●	29 (≈ 2%)
✓	✓	✓	✗	◐	11
✗	✓	–	✓	◐	2
✓	✗	–	✓	◐	132
✗	✗	–	✓	◐	117
				Total:	262 (≈ 20%)
✓	✗	✓	✗	○	354
✗	✗	✓	✗	○	482
✗	✓	✓	✗	○	3
✓	✓	✗	✗	○	2
✓	✗	✗	✗	○	67
✗	✓	✗	✗	○	2
✗	✗	✗	✗	○	126
				Total:	1036 (≈ 78%)
				Grand Total:	1327

[1] ● strong, ◐ weak, ○ inadequate

The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates.
  Makes affiliations recognizable and proofs identity.

The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates.
  Makes affiliations recognizable and proofs identity.
- Enable DNSSEC.
  Secures name resolution and avoids possible DV misissuance.

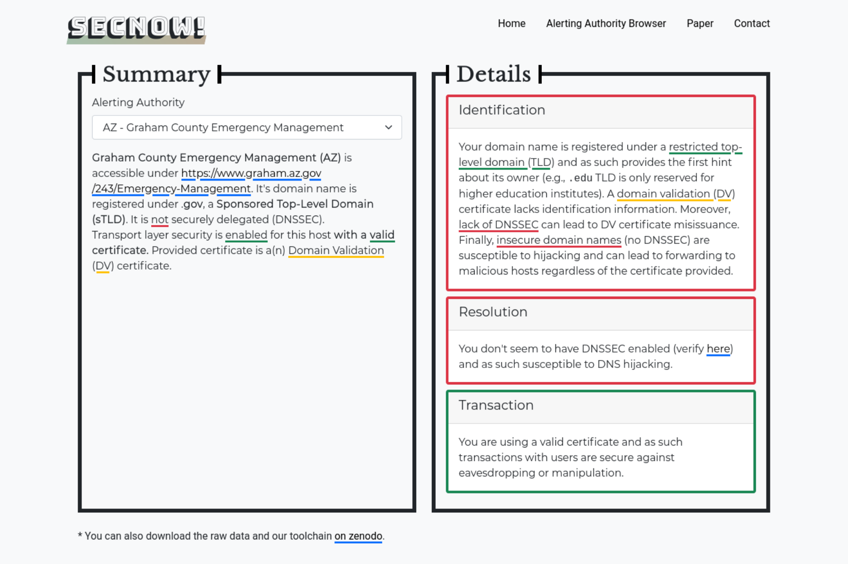
The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates.
  Makes affiliations recognizable and proofs identity.
- Enable DNSSEC.
  Secures name resolution and avoids possible DV misissuance.
- Consider TLSA domain issued certificates (DANE EE)
  Provides alternative to DV certificates.

The Road Ahead. Suggested Improvements for Alerting Authorities.

- Choose securely delegated names under restricted TLDs + OV/EV certificates.
  Makes affiliations recognizable and proofs identity.
- Enable DNSSEC.
  Secures name resolution and avoids possible DV misissuance.
- Consider TLSA domain issued certificates (DANE EE)
  Provides alternative to DV certificates.
- Use dedicated domain names and certificates.
  Avoids fate-sharing.

Data? More Details? Check out https://aa.secnow.net!



Summary

Alerting Authority

AZ - Graham County Emergency Management

Graham County Emergency Management (AZ) is accessible under https://www.graham.az.gov/243/Emergency-Management. It's domain name is registered under .gov, a **Sponsored Top-Level Domain (sTLD)**. It is not securely delegated (DNSSEC). Transport layer security is enabled for this host **with a valid certificate**. Provided certificate is a(n) Domain Validation (DV) certificate.

Details

Identification

Your domain name is registered under a restricted top-level domain (TLD) and as such provides the first hint about its owner (e.g., **.edu** TLD is only reserved for higher education institutes). A domain validation (DV) certificate lacks identification information. Moreover, lack of DNSSEC can lead to DV certificate misissuance. Finally, insecure domain names (no DNSSEC) are susceptible to hijacking and can lead to forwarding to malicious hosts regardless of the certificate provided.

Resolution

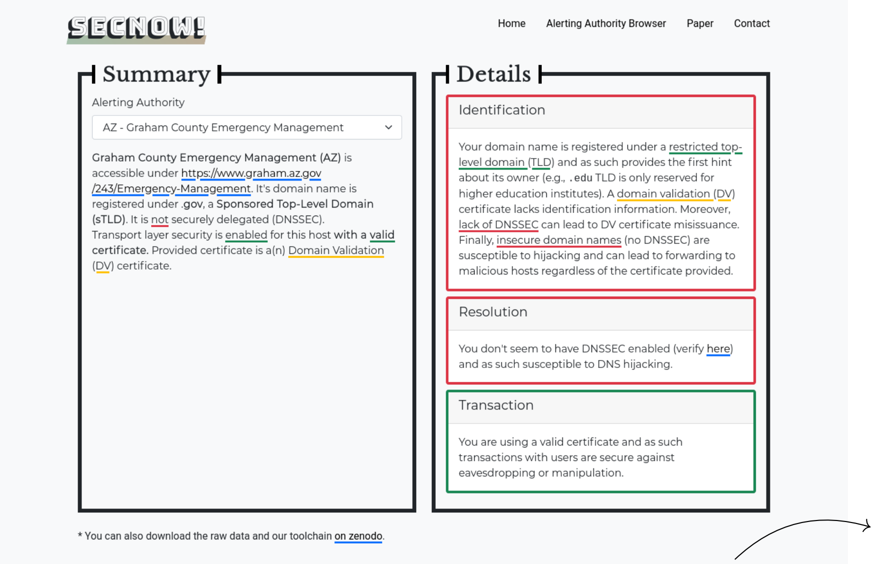
You don't seem to have DNSSEC enabled (verify here) and as such susceptible to DNS hijacking.

Transaction

You are using a valid certificate and as such transactions with users are secure against eavesdropping or manipulation.

* You can also download the raw data and our toolchain on zenodo.

Data? More Details? Check out `https://aa.secnow.net`!



Summary

Alerting Authority

AZ - Graham County Emergency Management

Graham County Emergency Management (AZ) is accessible under https://www.graham.az.gov/243/Emergency-Management. It's domain name is registered under **.gov**, a **Sponsored Top-Level Domain (sTLD)**. It is not securely delegated (DNSSEC). Transport layer security is enabled for this host **with a** valid **certificate**. Provided certificate is a(n) Domain Validation (DV) certificate.

Details

Identification

Your domain name is registered under a restricted top-level domain (TLD) and as such provides the first hint about its owner (e.g., `.edu` TLD is only reserved for higher education institutes). A domain validation (DV) certificate lacks identification information. Moreover, lack of DNSSEC can lead to DV certificate misissuance. Finally, insecure domain names (no DNSSEC) are susceptible to hijacking and can lead to forwarding to malicious hosts regardless of the certificate provided.

Resolution

You don't seem to have DNSSEC enabled (verify here) and as such susceptible to DNS hijacking.

Transaction

You are using a valid certificate and as such transactions with users are secure against eavesdropping or manipulation.

* You can also download the raw data and our toolchain on zenodo.

Question, critique, cooperation? `pft@acm.org`