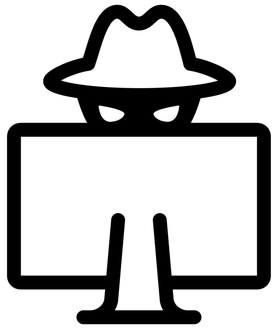
Využitie certifikátov a CT logov na komunikáciu

Študent: Matej Jurčák
Školiteľ: doc. RNDr. Martin Stanek, PhD.

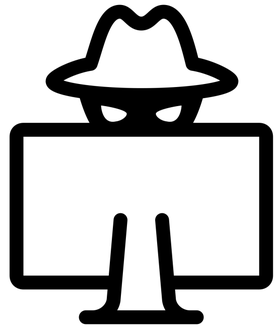
FAKULTA MATEMATIKY,
FYZIKY A INFORMATIKY
Univerzita Komenského
v Bratislave

CT kanál



Skrytý komunikačný kanál

CT logy + certifikáty



Skryté komunikačné kanály

uniba.sk | GEANT OV RSA CA 4 | USERTrust RSA Certification Authority

Subject Name

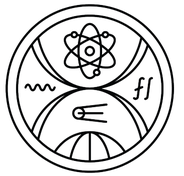
Country	SK
State/Province	Bratislavský kraj
Organization	Univerzita Komenského v Bratislave
Common Name	uniba.sk

Issuer Name

Country	NL
Organization	GEANT Vereniging
Common Name	GEANT OV RSA CA 4

Validity

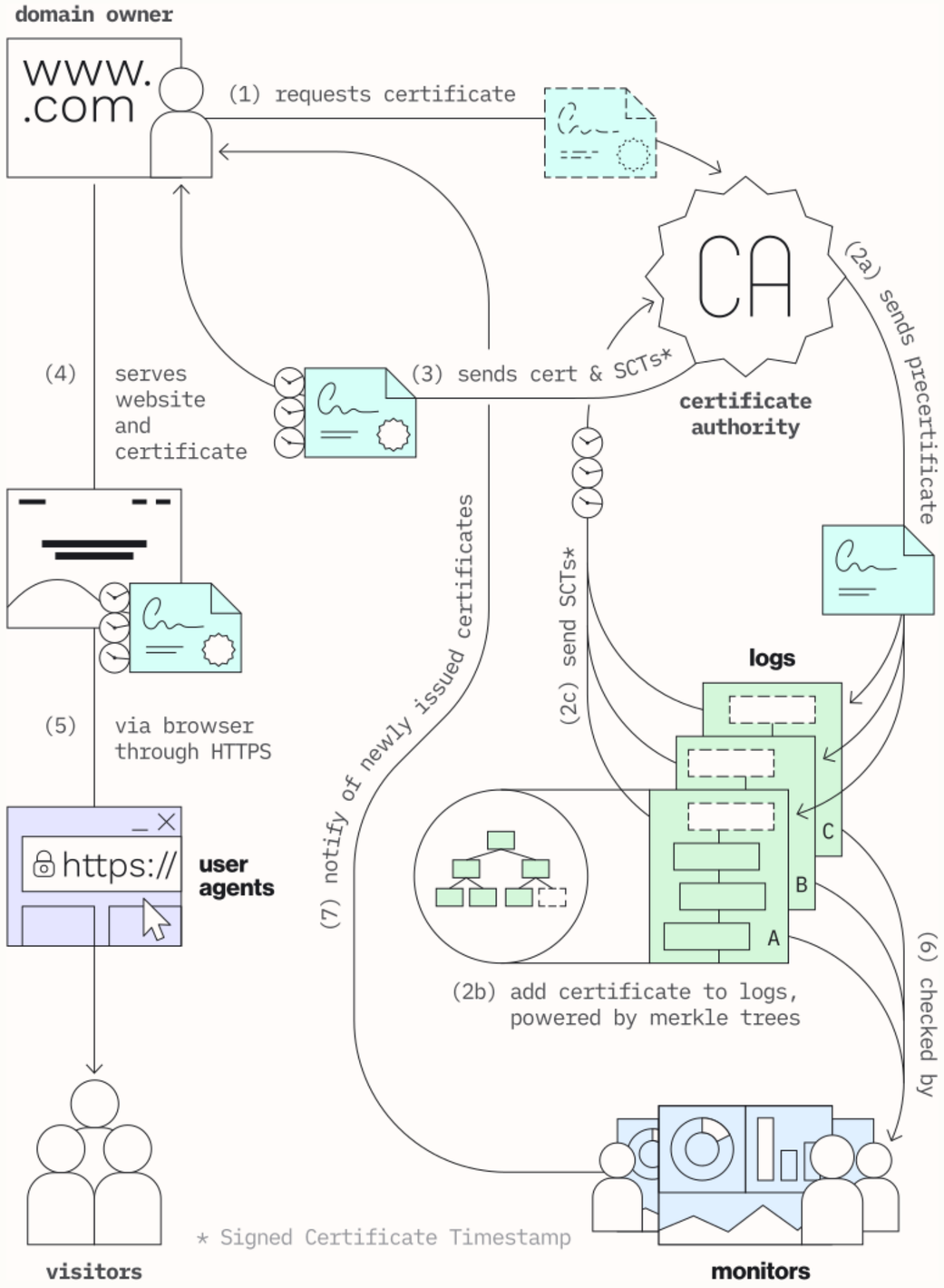
Not Before	Mon, 05 Jun 2023 00:00:00 GMT
Not After	Tue, 04 Jun 2024 23:59:59 GMT



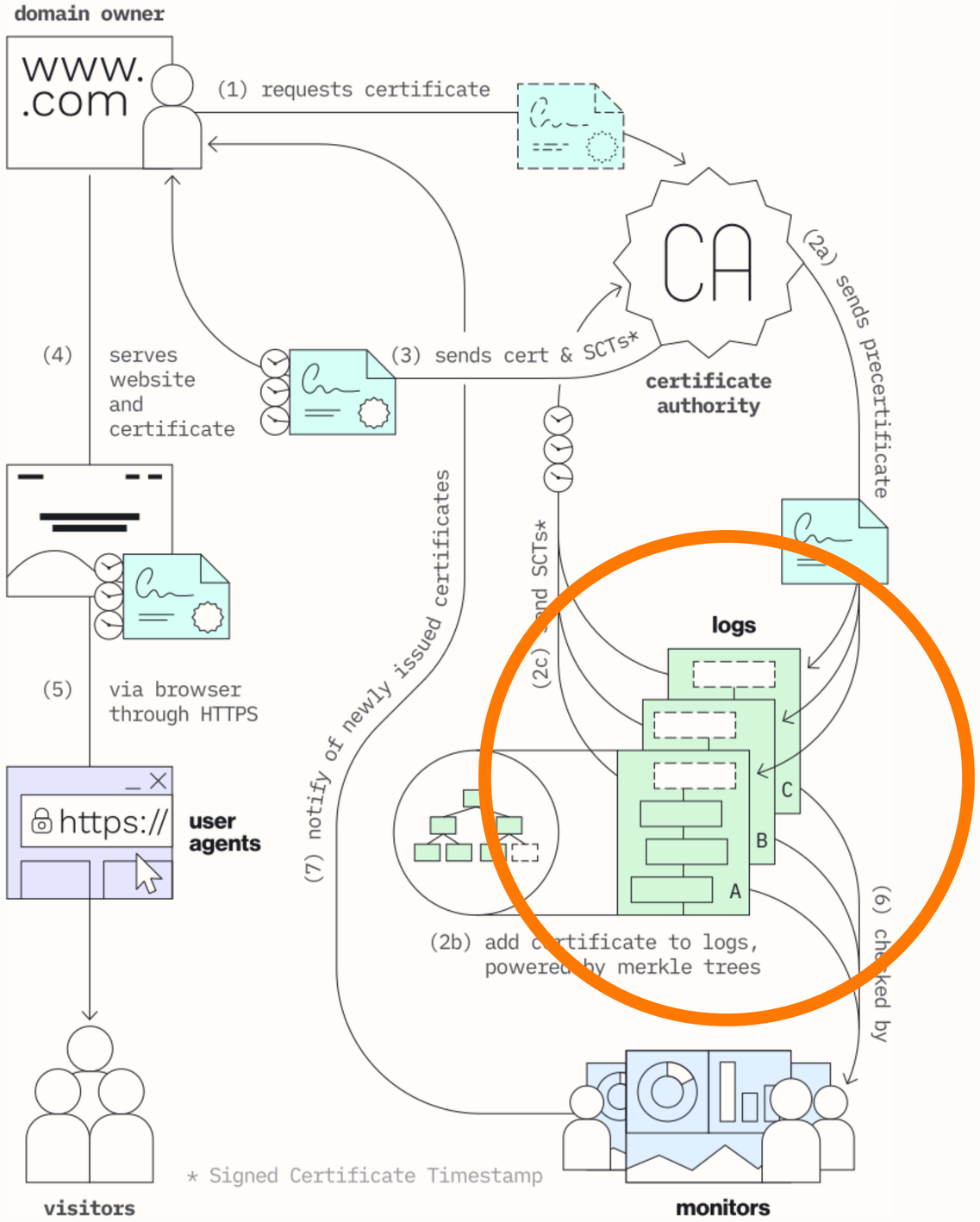
Certificate Transparency

Ekosystém, ktorý umožňuje transparentné a overiteľné vydávanie certifikátov webových stránok.

https://certificate.transparency.dev/



https://certificate.transparency.dev/howctworks/



https://certificate.transparency.dev/howctworks/

CT logy

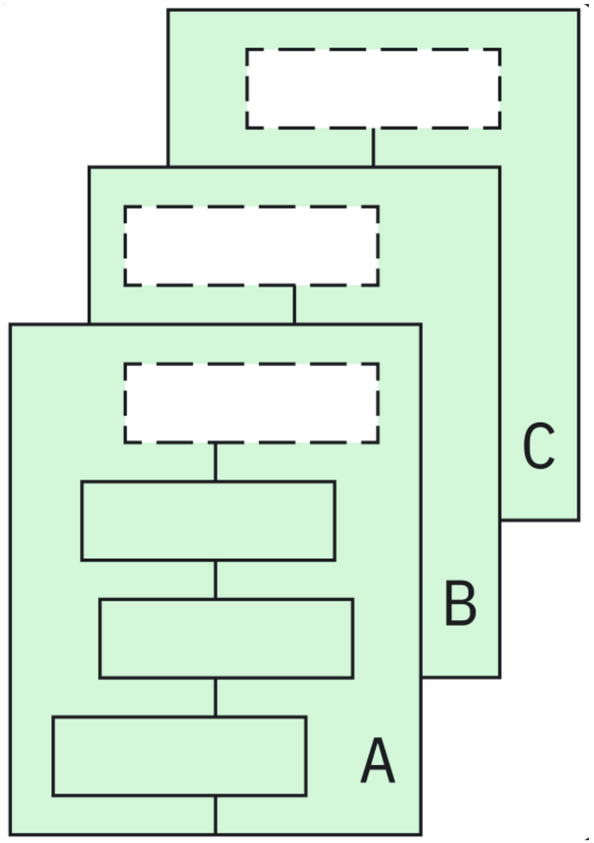
Certificate logs are **append-only** ledgers of certificates. Because they're distributed and independent, **anyone can query them** to see what certificates have been included and when.

https://certificate.transparency.dev/

Modelový scénar komunikácie

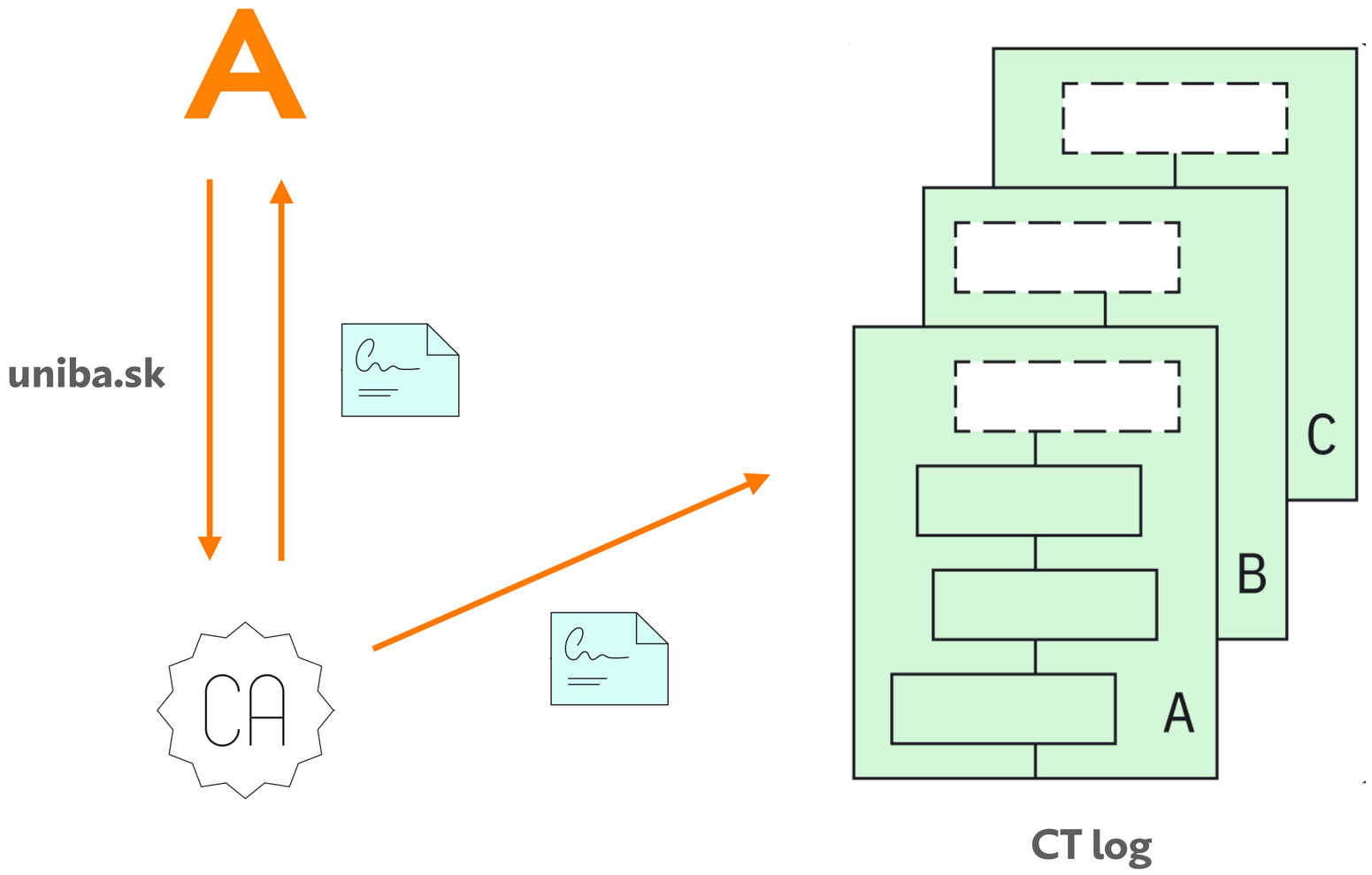
A

B

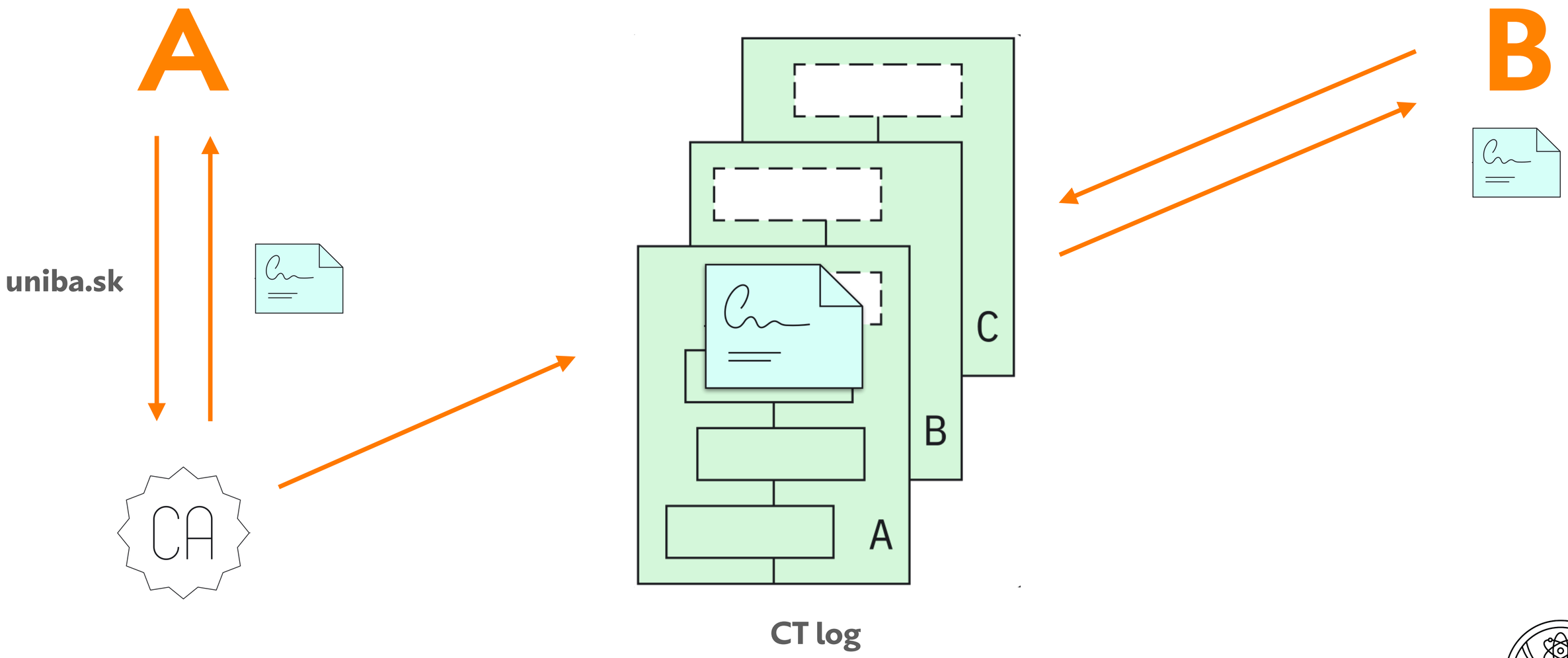


CT log

Modelový scénar komunikácie



Modelový scénar komunikácie



Modelový scénar komunikácie

- jednosmerná komunikácia
- útočník posiela príkazy malware-u (C&C útok)
- prijímateľ má k dispozícii len informáciu o doménovom mene
- šifrovaniu sa **ne**venujeme

- **skrytý kanál** → monitorovacie systémy majú v súčasnosti **nízku** motiváciu requesty na CT logy blokovať alebo analyzovať

Vkladanie správy do certifikátu

Vkladanie správy do certifikátu

- nad ktorými atribútmi certifikátu má žiadateľ kontrolu?

- Subject Name (SN): `uniba.sk`
- Subject Alternative Name (**SAN**): `[fmph.uniba.sk, fmed.uniba.sk, ...]`

Subject Alt Names

DNS Name	uniba.sk
DNS Name	cdv.uniba.sk
DNS Name	cusp.uniba.sk
DNS Name	druzba.uniba.sk
DNS Name	fedu.uniba.sk
DNS Name	fevth.uniba.sk
DNS Name	flaw.uniba.sk
DNS Name	fm.uniba.sk
DNS Name	fmed.uniba.sk
DNS Name	fmph.uniba.sk
DNS Name	fns.uniba.sk
DNS Name	fpharm.uniba.sk
DNS Name	fphil.uniba.sk
DNS Name	frcth.uniba.sk
DNS Name	fses.uniba.sk
DNS Name	fsport.uniba.sk

Vkladanie správy do certifikátu

Ako sa máš?.uniba.sk

Obmedzená znaková sada

Vkladanie správy do certifikátu

IFVW6IDTMEQG3Q5BYWQT6.uniba.sk

Kódovanie **Base32**

Vkladanie správy do certifikátu

JRXXEZLNEBUXA43VNUWCAYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF
6NVUSAZGDXJTGC3JB.uniba.sk

Dĺžka časti doménového mena **max. 63 znakov**

Vkladanie správy do certifikátu

JRXXEZLNE.BUXA43VNUWCAYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLR
F6NVUSAZGDXJTGC3JB.uniba.sk

Vkladanie správy do certifikátu

**BUXA43VNUWCAYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGD
XJTGC3JB.3UXA43VNUWCAYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF
6NVUSAZGDXJTGC3JB.3UXA43VNUWCAYLTOBX4LCBAGYZSA6TOMFVW65
RBEBLGLRF6NVUSAZGDXJTGC3JB.BUXA43VNUWCAYLTOBX4LCBAGYZSA
6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.**uniba.sk

Dĺžka doménového mena **max. 253 znakov**

Vkladanie správy do certifikátu

AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWCAY
LTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWCAYLT
OBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.BUXA43VNUWCAYLTOB
X4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.uniba.sk

BUXA43VNUWC.uniba.sk

Vkladanie správy do certifikátu

AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWCAY
LTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWCAYLT
OBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.BUXA43VNUWCAYLTOB
X4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.uniba.sk

HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.6FRHG33MYO5HI
3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.2FRHG33MYO5HI3T
FEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.IFRHG33MYO5HI3TFE
BXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.uniba.sk

Zachovanie poradia

Vkladanie správy do certifikátu

a1AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWC
AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWCAY
LTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.BUXA43VNUWCAYLT
OBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3.uniba.sk

a2HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.6FRHG33MYO5
HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.2FRHG33MYO5HI
3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.IFRHG33MYO5HI3T
FEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK.uniba.sk

Vkladanie správy do certifikátu

a1AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWC
AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.3UXA43VNUWCAY
LTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.BUXA43VNUWCAYLT
OBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3.uniba.sk

a2HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.6FRHG33MYO5
HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.2FRHG33MYO5HI
3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.IFRHG33MYO5HI3T
FEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK.uniba.sk

Časť d. mena musí začínať písmenom

Vkladanie správy do certifikátu

a1AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.x3UXA43VNUW
CAYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3J.x3UXA43VNUWCA
YLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3J.xBUXA43VNUWCAYL
TOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC.uniba.sk

a2HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.x6FRHG33MYO
5HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6.x2FRHG33MYO5H
I3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6.xIFRHG33MYO5HI3
TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2G.uniba.sk

Vkladanie správy do certifikátu

a1AYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3JB.x3UXA43VNUW
CAYLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3J.x3UXA43VNUWCA
YLTOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC3J.xBUXA43VNUWCAYL
TOBX4LCBAGYZSA6TOMFVW65RBEBLGLRF6NVUSAZGDXJTGC.uniba.sk

a2HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6D.x6FRHG33MYO
5HI3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6.x2FRHG33MYO5H
I3TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2GK6.xIFRHG33MYO5HI3
TFEBXGK3ODUFWSA3WDUFYGCZDZFQQMLPTFEBQWXQ55EB2G.uniba.sk

Limit na počet d. mien v atribúte SAN: **100** (LE)

Hľadanie certifikátu v CT logu

Vyhľadávanie v natívnych CT logoch

```
GET https://<log server>/ct/v1/get-entries

Inputs:

   start:  0-based index of first entry to retrieve, in decimal.

   end:  0-based index of last entry to retrieve, in decimal.

Outputs:

   entries:  An array of objects, each consisting of ...
```

Metódy vyhľadávania

- **crt.sh**

crt.sh (Certificate Search)

7447670234	2022-08-31	2022-08-31	2022-11-29	micro.dcs.fmph.uniba.sk	micro.dcs.fmph.uniba.sk
7447671419	2022-08-31	2022-08-31	2022-11-29	micro.dcs.fmph.uniba.sk	micro.dcs.fmph.uniba.sk
7407349671	2022-08-25	2022-08-25	2022-11-23	wiki.seclab.dcs.fmph.uniba.sk	wiki.seclab.dcs.fmph.uniba.sk
7407349659	2022-08-25	2022-08-25	2022-11-23	wiki.seclab.dcs.fmph.uniba.sk	wiki.seclab.dcs.fmph.uniba.sk
7395602106	2022-08-23	2022-08-23	2022-11-21	beda.dcs.fmph.uniba.sk	beda.dcs.fmph.uniba.sk
7395602368	2022-08-23	2022-08-23	2022-11-21	beda.dcs.fmph.uniba.sk	beda.dcs.fmph.uniba.sk
7330717154	2022-08-13	2022-08-13	2022-11-11	foja.dcs.fmph.uniba.sk	foja.dcs.fmph.uniba.sk
7330717107	2022-08-13	2022-08-13	2022-11-11	foja.dcs.fmph.uniba.sk	foja.dcs.fmph.uniba.sk

Metódy vyhľadávania

- **crt.sh**

  + poskytovanie viacerých funkcií, ktoré natívne logy nepodporujú (napr. vyhľadávanie pomocou doménového mena)

  - requesty mimo natívnych CT logov

  - nestabilnosť a nespoľahlivosť

Metódy vyhľadávania

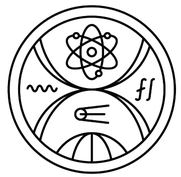
- **crt.sh**

  + poskytovanie viacerých funkcií, ktoré natívne logy nepodporujú (napr. vyhľadávanie pomocou doménového mena)

  - requesty mimo natívnych CT logov

  - nestabilnosť a nespoľahlivosť

- dodatočná informácia, ktorú bude mať prijímateľ → **čas odoslania prvej správy**
- odosielateľ v i. správe zahrnie informáciu o čase poslania i + 1. správy



Metódy vyhľadávania

- **crt.sh**

  + poskytovanie viacerých funkcií, ktoré natívne logy nepodporujú (napr. vyhľadávanie pomocou doménového mena)

  - requesty mimo natívnych CT logov

  - nestabilnosť a nespoľahlivosť

- **Binárne vyhľadávanie**

Binárne vyhľadávanie

Tabuľka 2.1: Úsek certifikátov z CT logu `argon2023`

Log ID	Not before	Domain names
1058068821	2023-05-07 09:04:53	www.expressiveverticals.com
1058068822	2023-05-07 09:05:01	www.swpowersystems.net,swpowersystems.net
1058068823	2023-05-07 09:04:56	www.milk.furniture
1058068824	2023-05-07 09:04:56	*.crumpling-crier.click,crumpling-crier.click
1058068825	2023-05-07 09:05:00	vikingflowerpatch.com
1058068826	2023-05-07 09:04:52	stockholmykt.ru,www.stockholmykt.ru
1058068827	2023-05-07 09:04:53	*.partner-massage.net,partner-massage.net

Metódy vyhľadávania

- **crt.sh**

  + poskytovanie viacerých funkcií, ktoré natívne logy nepodporujú (napr. vyhľadávanie pomocou doménového mena)

  - requesty mimo natívnych CT logov

  - nestabilnosť a nespoľahlivosť

- **Binárne vyhľadávanie**
- **Sekvenčné prehľadávanie**

Manuálne nahratie certifikátu do CT logu

```
POST https://<log server>/ct/v1/add-chain

Inputs:

   chain:  An array of base64-encoded certificates.  The first
      element is the end-entity certificate; the second chains to the
      first and so on to the last, which is either the root
      certificate or a certificate that chains to a known root
      certificate.
```

Priepustnosť CT kanála (Let's Encrypt)

$$\mathsf{CRT} = 50 \text{ certifikátov/týždeň}$$

$$\mathsf{SAN} = 100 \text{ domén/certifikát}$$

$$\mathsf{DN} = 253 \text{ bajtov/doména}$$

$$\mathsf{P} = \mathsf{CRT} \cdot \mathsf{SAN} \cdot \mathsf{DN} = \mathbf{1,265} \ \frac{\mathsf{MB}}{\text{týždeň}}$$

Komponenty CT kanála

- **Python**

- `send_message.py` (odosielateľ) — zakóduje správu, vloží do atribútu SAN a požiada o certifikát
- `add_chain.py` (odosielateľ) — manuálne vloží certifikát do CT logu
- `receive_message.py` (prijímateľ) — sekvenčne prehľadáva vybraný CT log až kým nenájde hľadaný certifikát.

Implementácia `send_message.py`

Posielanie žiadosti / Validácia doménových mien

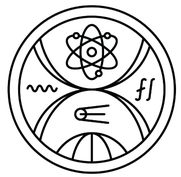
- protokol ACME, softvér **certbot**
- validácia doménových mien → **úprava DNS záznamov:**

```
_acme-challenge.ctlr.seclab.dcs.fmph.uniba.sk. 300 IN TXT “gfj9Xq…Rg85nM"
```

- štandardne je požiadanie o certifikát pomocou certbota interaktívne (v termináli), vrámci automatizácie tomu zabraňujeme

Implementácia `receive_message.py`

- aktuálna veľkosť logu → **`/get-sth`**
- prehľadávanie:
  - **`/get-entries <index, index + max_block_size>`** → `max_block_size` obsahuje maximálny počet záznamov, ktoré CT log vráti pre jeden request.
  - záznam dekóduje a vytiahne z neho SAN
  - skontroluje, či sa v atribúte SAN nenachádza vopred dohodnuté doménové meno. Ak nie, posunie sa na ďalší úsek a proces zopakuje.



Ukážka funkčnosti konceptu

receive_message.py

```
$ python receive_message.py ctlr.seclab.dcs.fmph.uniba.sk --log-name argon2023

Looking for certificate inside argon2023 from index 1076325998.

1076326000 | 2023-06-20 09:59:56 | shop.humask.com
1076326002 | 2023-06-20 09:59:59 | lockedroomcrafts.com
...
...
...
1076326160 | 2023-06-20 10:00:02 | www.halfchuboutfitters.com
1076326162 | 2023-06-20 10:00:00 | ctlr.seclab.dcs.fmph.uniba.sk,
    a0JETW2IDTMVXGI2LOM4QGCIDNMVZXGYLHMUQHI2DSN52WO2BAORUGKICDKQQGG.
    x2DBNZXGK3BOEBESA53JNRWCA43FNZSCAYLON52GQZLSEBXW4ZJAN5XCAMZQFY3.
    xC4MRQGIZSAYLUEA4TUMBQHIYDAICVKRBS4.ctlr.seclab.dcs.fmph.uniba.sk

Successfully found the message sent through the CT channel: I'm sending a message
    through the CT channel. I will send another one on 30.6.2023 at 9:00:00 UTC.
```

OTÁZKY
PRIPOMIENKY

Vedeli by ste uviesť korektnejší odhad maximálnej priepustnosti CT kanála so zohľadnením uvedených pripomienok a zahrnutím nejakej realistickej dĺžky registrovaného doménového mena?

$$|S_{b32}| = \left\lceil \frac{|S|}{5} \right\rceil \cdot 8$$

Kódovanie **Base32**

$$\begin{aligned} \mathsf{RD} &= \text{uniba.sk} \\ \mathsf{CRT} &= 50 \text{ certifikátov/týždeň} \\ \mathsf{SAN} &= 100 \text{ domén/certifikát} \\ \mathsf{DN_{RN}} &= 237 \text{ bajtov/doména} \end{aligned}$$

$$\mathsf{P_{b32}} = \mathsf{CRT} \cdot \mathsf{SAN} \cdot \mathsf{DN} = \mathbf{1,19} \ \frac{\mathsf{MB}}{\text{týždeň}}$$

$$\mathsf{P} = \left\lceil \frac{\mathsf{P_{b32}}}{8} \right\rceil \cdot 5 = \mathbf{0,74} \ \frac{\mathsf{MB}}{\text{týždeň}}$$

Ako problém spomínate, že Let's Encrypt asi do CT logu nahráva len predcertifikáty. Prečo sa predcertifikáty nedajú tiež použiť na prijatie správy? Predsa uvádzate, že obsahujú rovnaké informácie ako certifikáty (len s rozšírením navyše).

Ako problém spomínate, že Let's Encrypt asi do CT logu nahráva len predcertifikáty. Prečo sa predcertifikáty nedajú tiež použiť na prijatie správy? Predsa uvádzate, že obsahujú rovnaké informácie ako certifikáty (len s rozšírením navyše).

Dajú sa použiť.