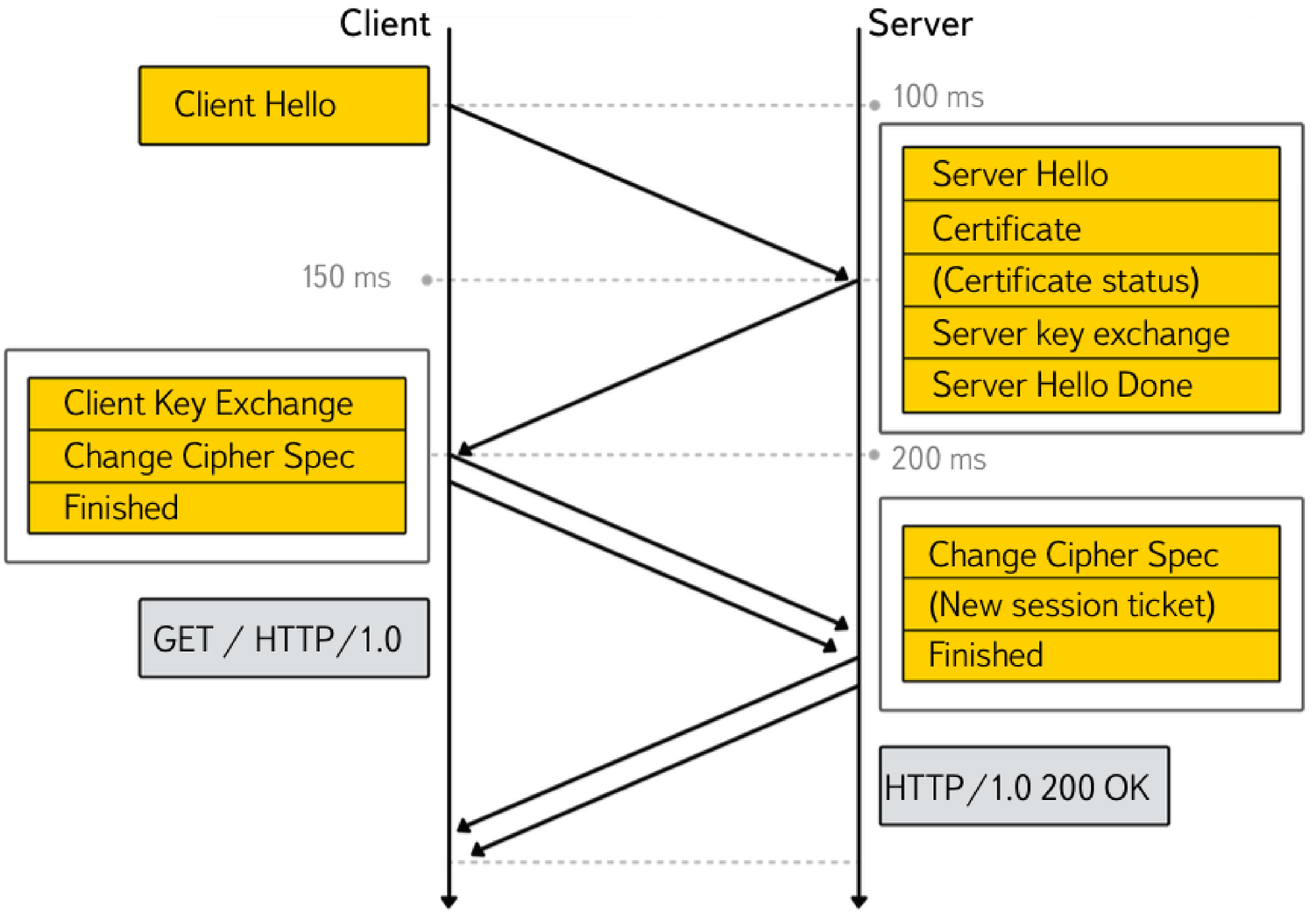
Yandex

Certificate Transparency FTW

Eldar Zaitov

Transport Layer Security

TLS Handshake

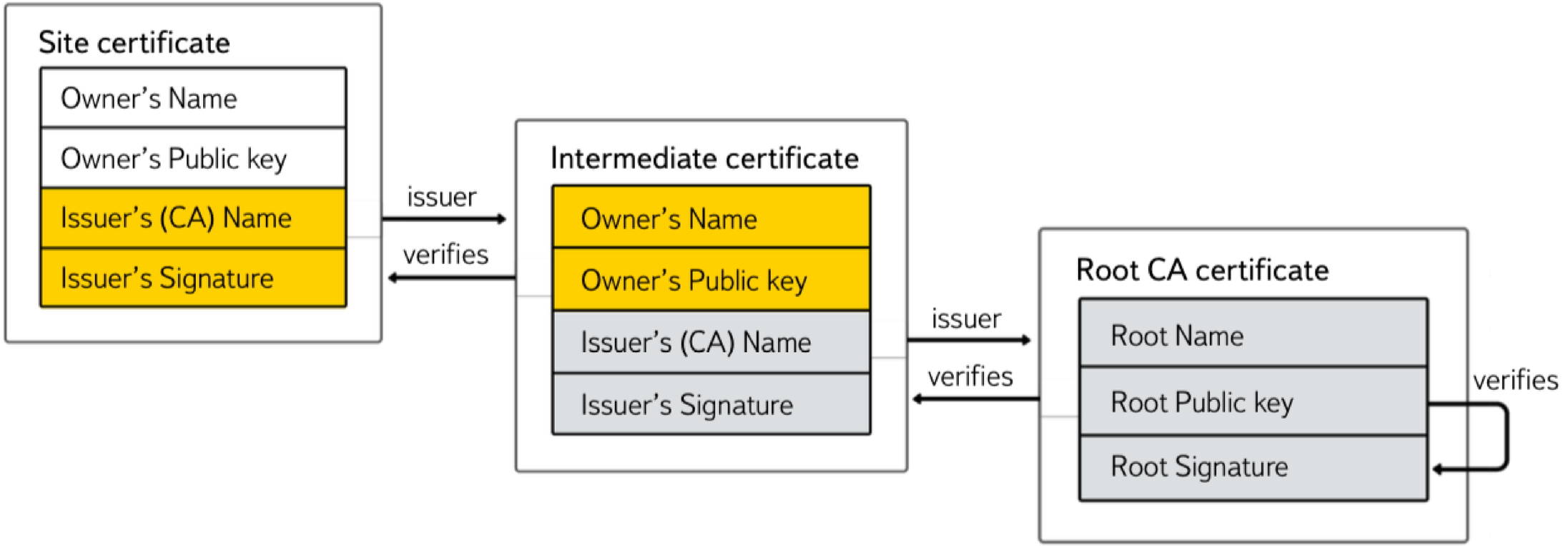


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            25:df:9c:48:86:b7:b8:cc:88:15:ad:6a:69:c4:7e:30
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=RU, O=Yandex LLC, OU=Yandex Certification
Authority, CN=Yandex CA
        Validity
            Not Before: Dec 10 13:42:33 2015 GMT
            Not After : Dec  9 13:42:33 2017 GMT
        Subject: C=RU, O=Yandex LLC, OU=ITO, L=Moscow, ST=Russia,
CN=yandex.ru
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
…
```

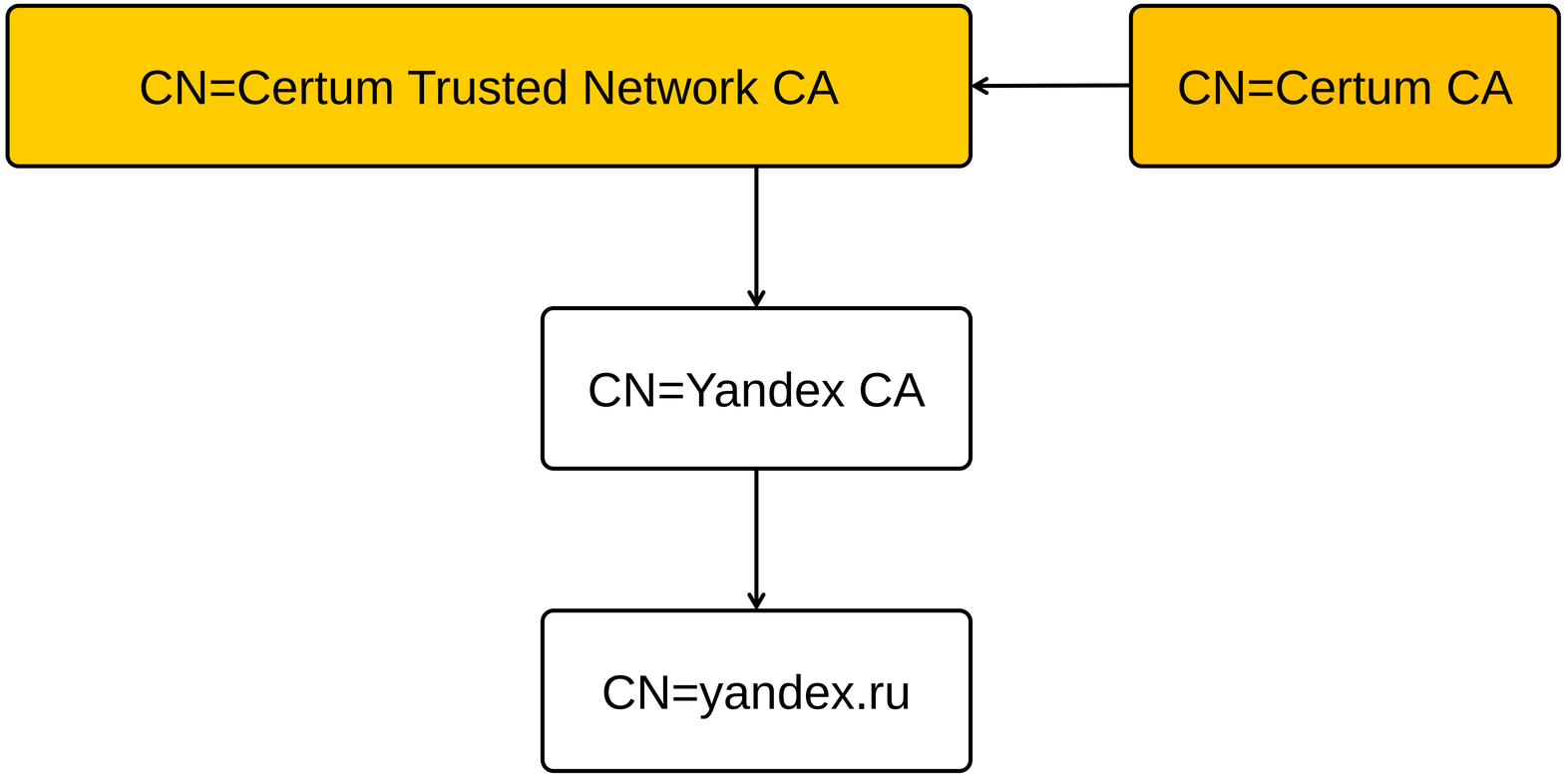
```
…
X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
Authentication
            Netscape Cert Type:
                SSL Client, SSL Server
            X509v3 Subject Alternative Name:
                DNS:yandex.net, DNS:m.yandex.ua, DNS:yandex.com.tr,
DNS:yandex.kz, DNS:www.yandex.ua, DNS:www.yandex.kz, DNS:yandex.ua,
DNS:yandex.by, DNS:www.yandex.ru, DNS:video.yandex.kz,
DNS:images.yandex.by, …

 Signature Algorithm: sha256WithRSAEncryption
         7a:08:37:bd:9c:7b:a1:6e:a2:96:af:ad:d9:78:5d:87:cf:96:
         …
```

Certificate Authority



Yandex Certificate Authority



PKI is fragile

COMODO RSA Certification Au...	COMODO RSA Certification Auth...	19.01.2038	Проверка подлинности с...	COMODO SECURE™
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	01.01.2038	Проверка подлинности с...	Go Daddy Root Cer...
Starfield Root Certificate Autho...	Starfield Root Certificate Authorit...	01.01.2038	Проверка подлинности с...	Starfield Root Certif...
GeoTrust Primary Certification ...	GeoTrust Primary Certification Au...	02.12.2037	Проверка подлинности с...	GeoTrust Primary C...
thawte Primary Root CA - G3	thawte Primary Root CA - G3	02.12.2037	Проверка подлинности с...	thawte Primary Roo...
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	02.12.2037	Проверка подлинности с...	VeriSign Universal R...
StartCom Certification Authority	StartCom Certification Authority	17.09.2036	Проверка подлинности с...	StartCom Certificati...
thawte Primary Root CA	thawte Primary Root CA	17.07.2036	Проверка подлинности с...	thawte
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17.07.2036	Проверка подлинности с...	VeriSign
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23.03.2036	<Все>	Microsoft Root Cert...

130+ Microsoft Trusted Root Certificate Program Participants

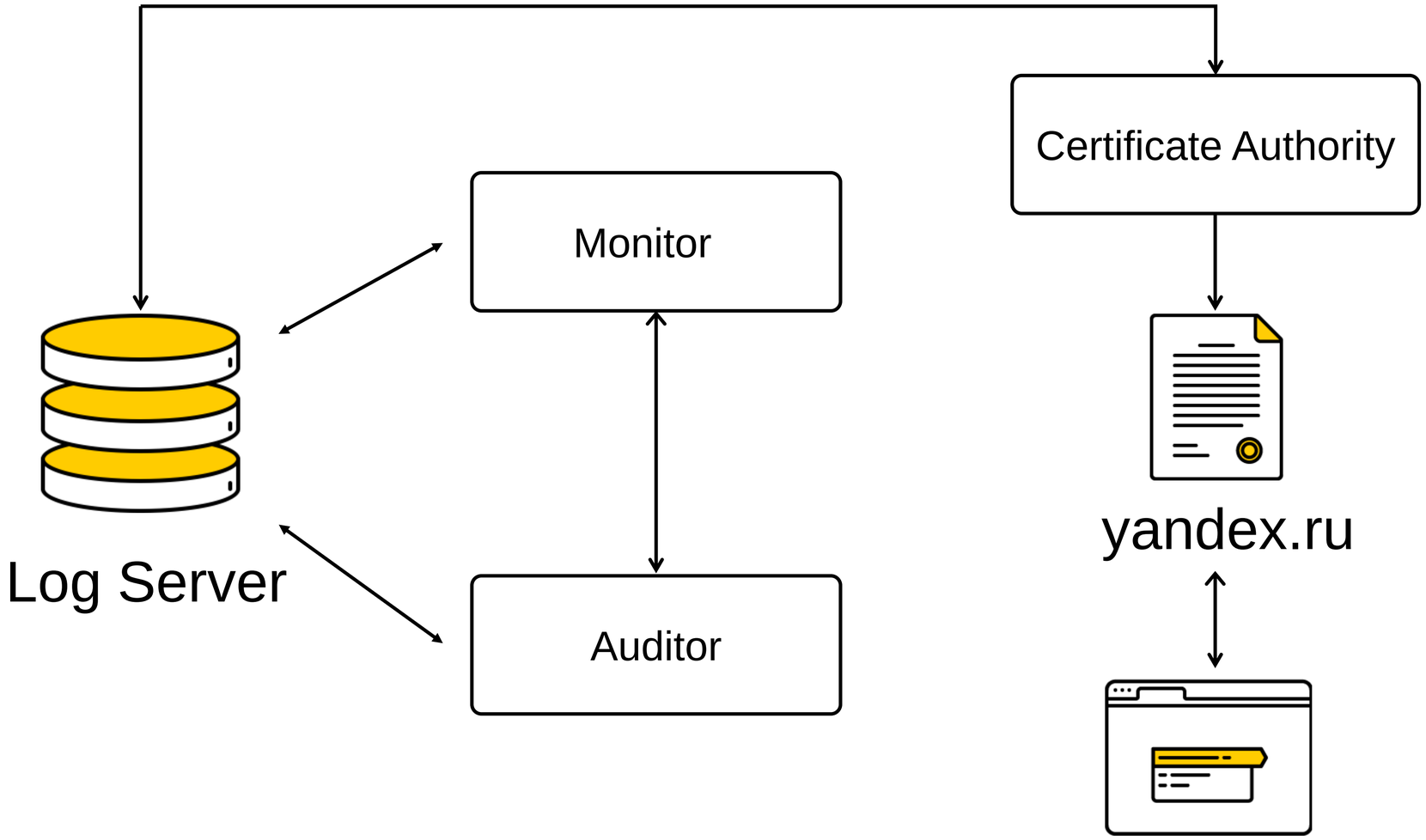
Fraudulent and unauthorized certificates

- DigiNotar, 2011
- TrustWave, CNNIC, TURKTRUST, …

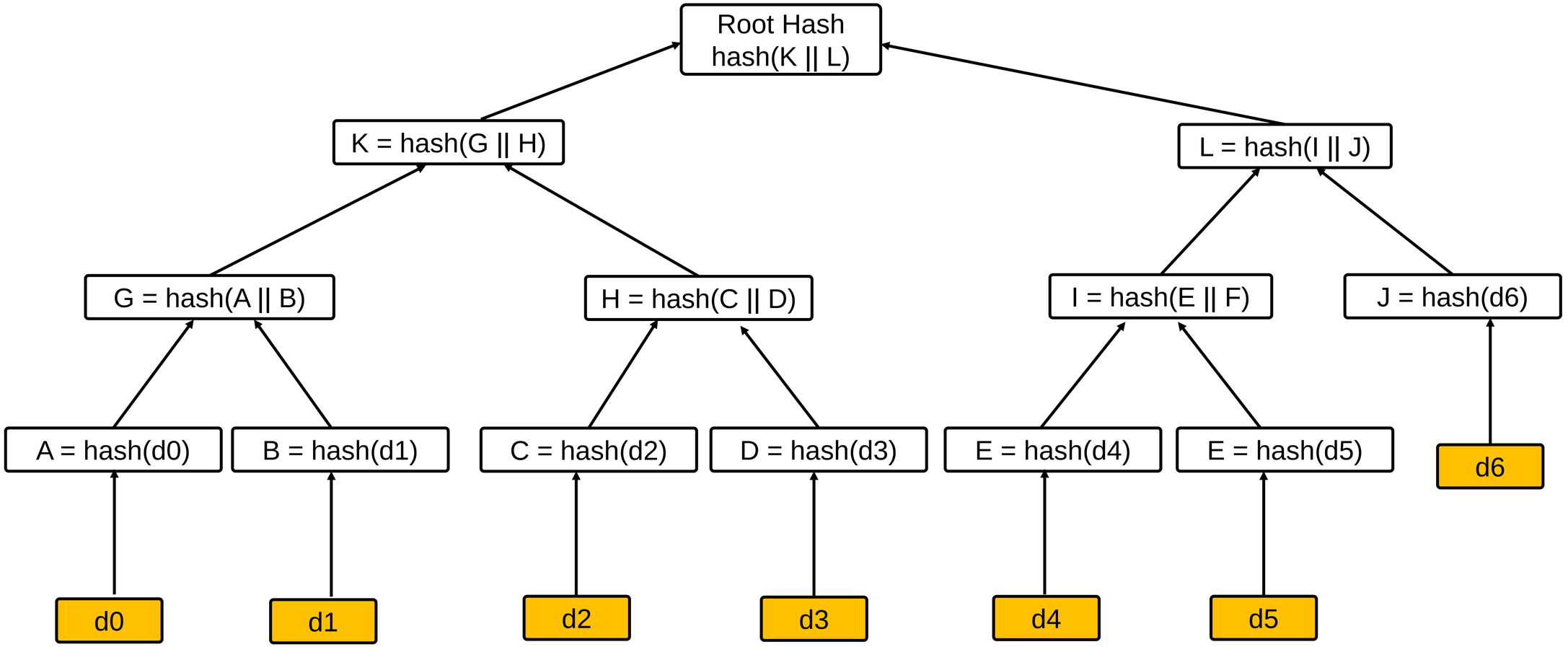
Certificate Pinning

- **TACK** (M.Marlinspike, T.Perrin)
- **DANE TLSA** (RFC6698)
- **HTTP Public Key Pinning** (RFC7469, R.Sleevi, C.Palmer, C.Evans)

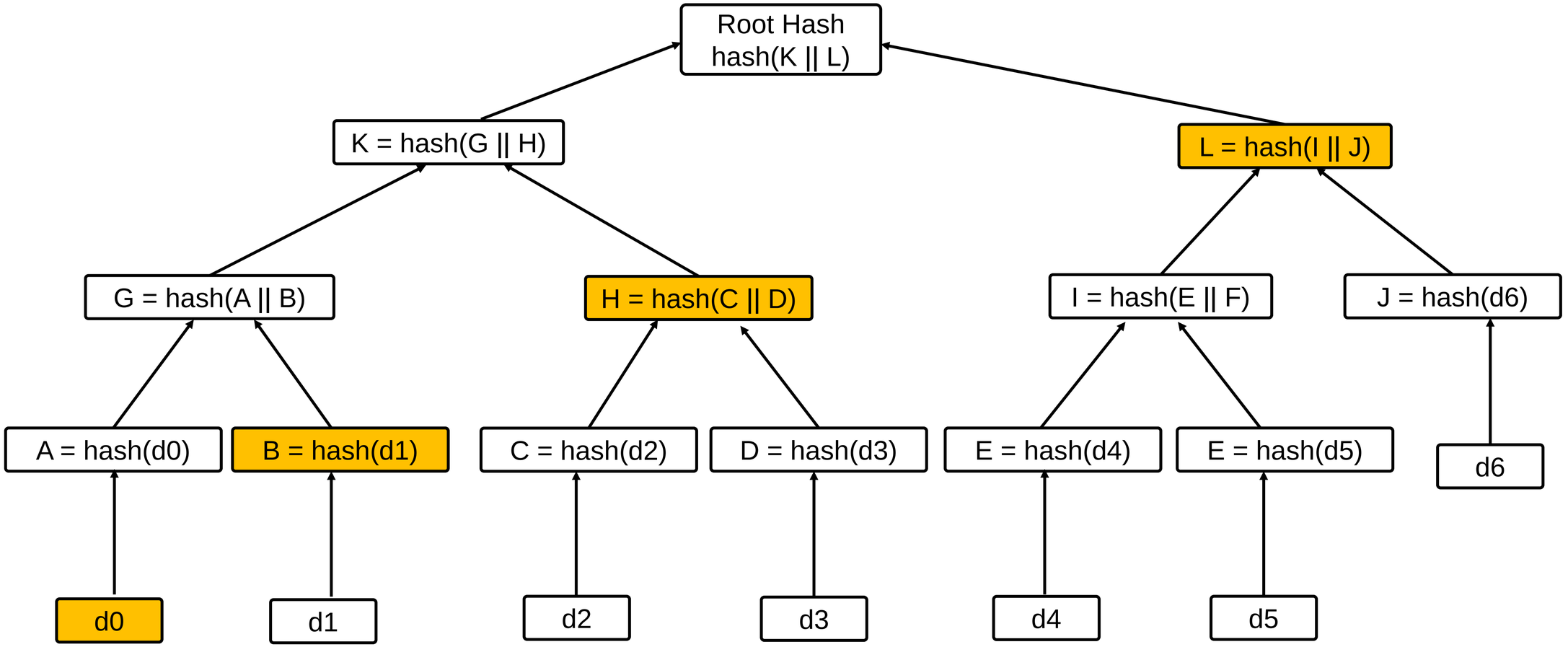
Certificate Transparency (RFC6962)



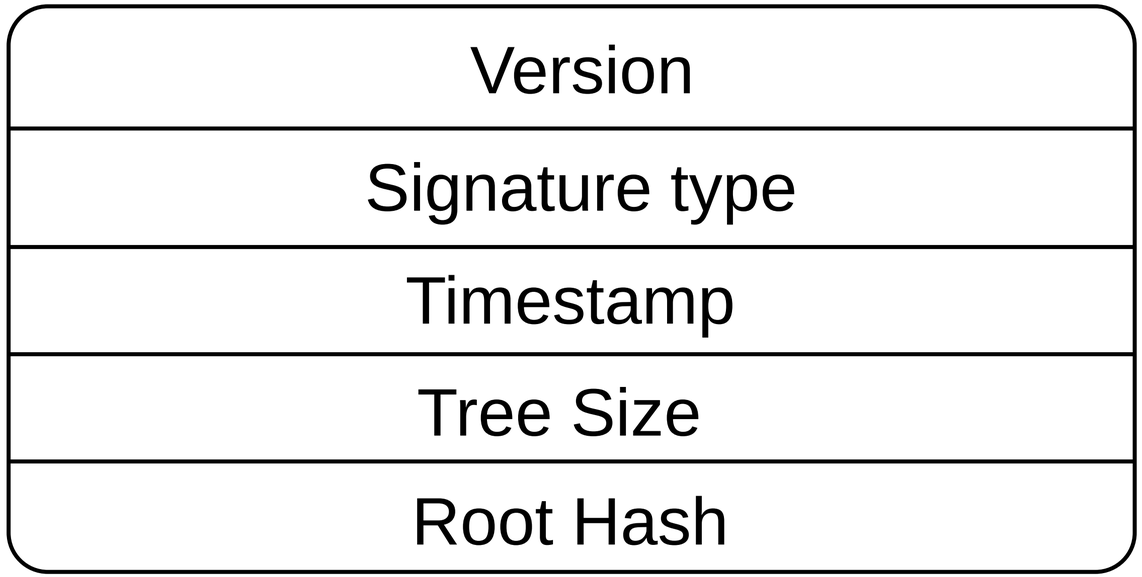
Merkle Tree


Root Hash
hash(K || L)
K = hash(G || H)
L = hash(I || J)
G = hash(A || B)
H = hash(C || D)
I = hash(E || F)
J = hash(d6)
A = hash(d0)
B = hash(d1)
C = hash(d2)
D = hash(d3)
E = hash(d4)
E = hash(d5)
d6
d0
d1
d2
d3
d4
d5

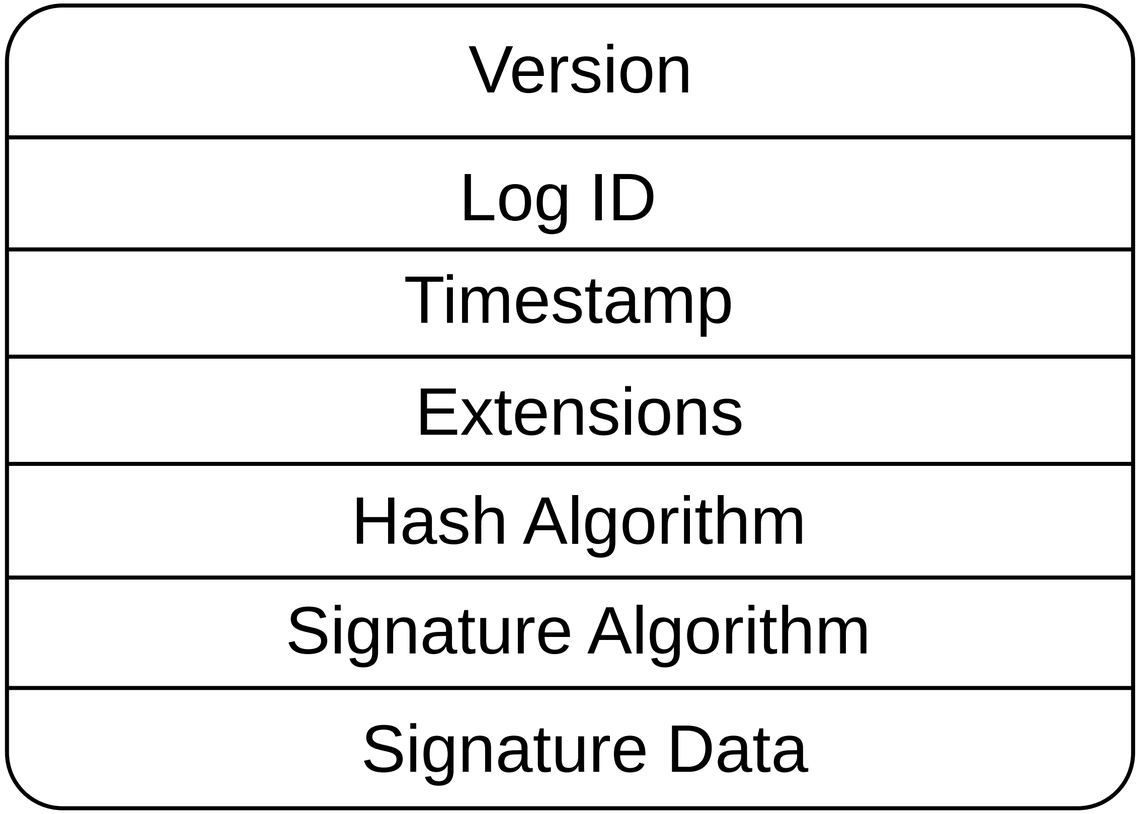
Merkle Tree


Root Hash
hash(K || L)
K = hash(G || H)
L = hash(I || J)
G = hash(A || B)
H = hash(C || D)
I = hash(E || F)
J = hash(d6)
A = hash(d0)
B = hash(d1)
C = hash(d2)
D = hash(d3)
E = hash(d4)
E = hash(d5)
d6
d0
d1
d2
d3
d4
d5

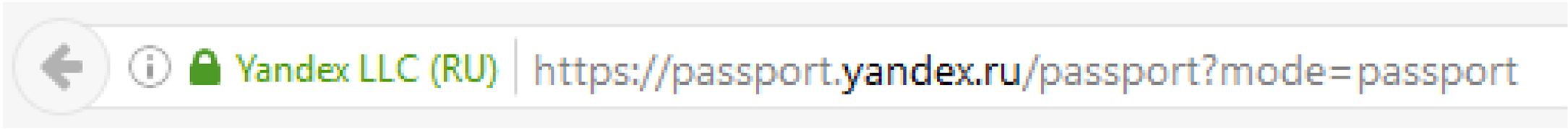
Signed Tree Head

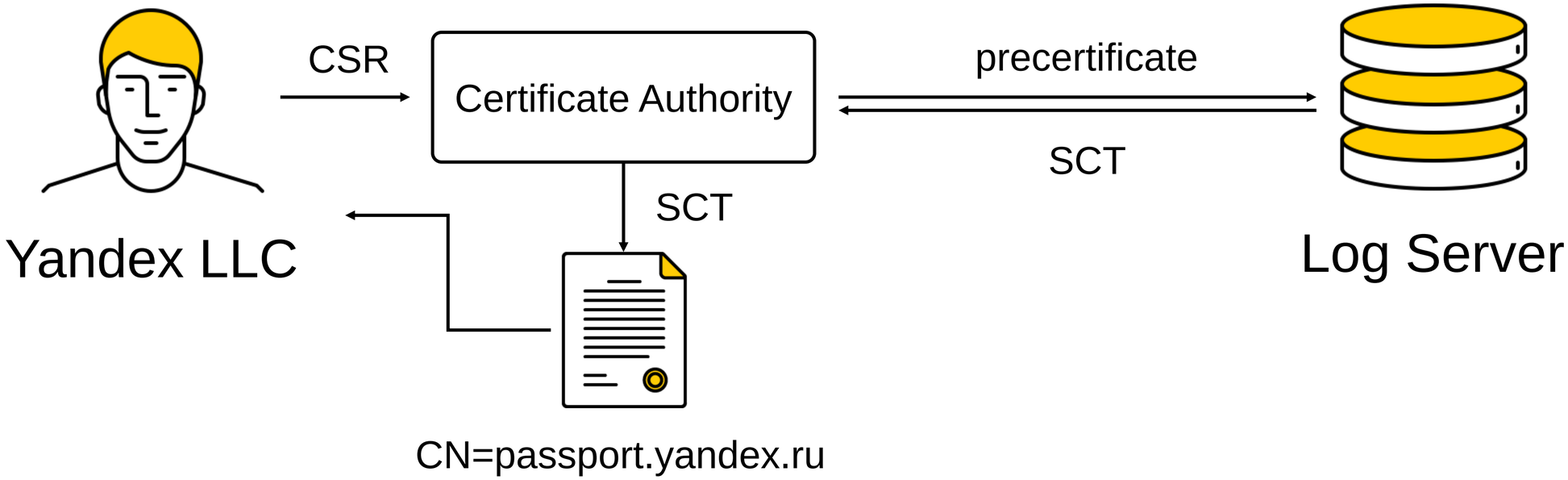


Signed Certificate Timestamp



Certificate Transparency for EV





```
…
Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Extended Validation
CA - SHA256 - G2
Subject: businessCategory=Private
Organization/serialNumber=1027700229193/1.3.6.1.4.1.311.60.2.1.3=RU/1
.3.6.1.4.1.311.60.2.1.2=Moscow, C=RU, ST=Moscow, L=Moscow/street=16,
Leo Tolstoy St., OU=ITO, O=Yandex LLC, CN=passport.yandex.ru
…
        X509v3 Subject Alternative Name:
            DNS:passport.yandex.ru, DNS:passport.yandex.by,
DNS:passport.yandex.com, DNS:passport.yandex.com.tr,
DNS:passport.yandex.kz, …

        1.3.6.1.4.1.11129.2.4.2:
                ...V.T.v.h....d..:...(.L.qQ]g..D. …
```

CT in real world

Symantec (www.google.com / google.com)

2015-09-23	2015-09-23	C=US, O=Google Inc, CN=Google Internet Authority G2
2015-09-14	2015-09-14	C=US, O="thawte, Inc.", CN=thawte EV SSL CA - G3
2015-09-09	2015-09-09	C=US, O=Google Inc, CN=Google Internet Authority G2
2015-09-09	2015-09-09	C=US, O=Google Inc, CN=Google Internet Authority G2
2015-08-26	2015-08-26	C=US, O=Google Inc, CN=Google Internet Authority G2
2015-08-26	2015-08-26	C=US, O=Google Inc, CN=Google Internet Authority G2
2015-08-12	2015-08-12	C=US, O=Google Inc, CN=Google Internet Authority G2

CT in real world

Let’s Encrypt (*.fb.com)

Criteria	Identity LIKE '%.fb.com'

Certificates

Logged At	Not Before	Identity	Iss
2016-04-23	2016-04-12	*.fb.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High As
2016-04-23	2016-04-22	investor.fb.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2016-04-16	2016-04-13	facebook360.fb.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High As
2016-04-14	2016-04-09	messengerplatform.fb.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High As
2016-04-14	2016-04-09	www.messengerplatform.fb.com	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High As

CT vs Phishing

mail-yandex-id-login-notification.ru	Let's Encrypt Authority X3	**mail-yandex-id-login-notification.ru**, **www.mail-yandex-id-login-notification.ru**	2016-04-19 14:13:00	2016-07-18 14:13:00
sni26838.cloudflaressl.com	COMODO ECC Domain Validation Secure Server CA 2	sni26838.cloudflaressl.com, *.bridgwatercarnival.org.uk, *.care.com.ng, *.cdmc-sw.co.uk, *.dolar.xyz, *.funnyafricanjokes.com, *.hinkleysupplychain.co.uk, *.hometutorsinlagos.com, *.llstn.com, *.nulledcontent.com, *.prepclass.com.ng, *.pvcjm.com, *.sendsmslive247.com, *.stolencouchgames.com, ***.tolokayandex.com**, *.towncouncilwebsite.co.uk, *.whiteknightmarketing.co.uk, *.wordsee.info, *.y0la.com, bridgwatercarnival.org.uk, care.com.ng, cdmc-sw.co.uk, dolar.xyz, funnyafricanjokes.com, hinkleysupplychain.co.uk, hometutorsinlagos.com, llstn.com, nulledcontent.com, prepclass.com.ng, pvcjm.com, sendsmslive247.com, stolencouchgames.com, **tolokayandex.com**, towncouncilwebsite.co.uk, whiteknightmarketing.co.uk, wordsee.info, y0la.com	2016-04-17 00:00:00	2016-10-23 23:59:59

https://github.com/kyprizel/ct_mon/

Thank you for your attention!
Questions?

Contacts

Eldar Zaitov

 kyprizel

 ezaitov@yandex-team.ru