ОТЧЕТ
ПО РЕЗУЛЬТАТАМ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

РАСШИРЕНИЯ TLS-СЕРТИФИКАТОВ В ГРУППЕ СТАНДАРТОВ X.509

Июль 2017 года

ВВЕДЕНИЕ

Под расширениями TLS-сертификатов (далее - сертификатов) в группе стандартов X.509 понимаются поля и структуры данных, которые, в общем случае, являются необязательными, но могут входить в состав сертификата и дополнять его специальной информацией, определяющей параметры или порядок использования сертификата. В общем случае, возможны произвольные по информационному наполнению расширения, если их представление не противоречит формату данных сертификата. На практике, широко используемые расширения, так или иначе, стандартизованы, а сертификат, подписываемый хорошо известным удостоверяющим центром (УЦ), будет содержать лишь те расширения, которые допущены данным УЦ к использованию (см. блок «Обзор расширений сертификатов X.509» ниже).

При этом если формально сертификат может не содержать ни одного расширения, на практике современный валидный сертификат в обязательном порядке содержит их несколько. В частности, расширения необходимы для корректного определения допустимых способов использования ключа, указанного в сертификате, для корректного сопоставления имён, а также в целом ряде других случаев.

Таким образом, расширения играют определяющую роль в практическом использовании сертификатов.

ВЫБОРКА ДАННЫХ

Предметом настоящего исследования являются некоторые расширения X.509, обнаруживаемые в сертификатах, возвращаемых TLS-узлами, которые адресуются именами второго уровня в российских зонах .RU, .SU, .РФ.

Целями исследования являются:

- выяснение характеристик встреченных расширений, числовых характеристик структуры распределения расширений между прикладными аспектами протокола TLS. Как разбиваются исследуемые X509-расширения в имеющейся выборке по различным удостоверяющим центрам, как параметры расширений связаны с TLS-узлами, каковы характеристики распространённости тех или иных значений параметров;

- построение статистики распространённости расширений и параметров, которые

используются внутри расширений; обнаружение возможных аномалий.

Так как это поисковое исследование, каких-то узких гипотез, подлежащих проверке, не формулировалось.

Сбор сертификатов проводился с узлов, доступных по протоколу TCP на номере порта 443, что, на уровне приложений, соответствует протоколу HTTPS - основному защищённому транспорту веба.

Мы рассматриваем не все встреченные расширения, а только наиболее значимые, взятые из валидных сертификатов. В основном исследование касается серверных сертификатов (то есть, сертификатов, относящихся непосредственно к открытому ключу аутентифицируемого TLS-узла). Некоторые данные относятся и к серверным, и к сертификатам удостоверяющих центров. Там, где различие между типами сертификатами важно, типы обозначаются отдельно. Данный подход охватывает ключевые моменты прикладного использования протокола TLS в актуальном состоянии: аутентификация сторон (сервера) и выстраивание цепочки доверия с привлечением дополнительного источника информации о сертификатах (расширение Certificate Transparency SCT, см. ниже).

Внутри сертификатов расширения представлены специальными идентификаторами (OID), которые уникальны для каждого расширения. Однако непосредственное использование OID затрудняет изложение, поэтому для ясности мы используем в качестве названий расширений соответствующие текстовые строки из библиотек OpenSSL.

ОБЗОР РАСШИРЕНИЙ СЕРТИФИКАТОВ X.509

Разнообразие возможных расширений TLS-сертификатов велико. Среди них есть устаревшие расширения, например, Netscape Revocation Url или Netscape Base Url, которые уже не встречаются в валидных сертификатах. Существуют и чрезвычайно важные расширения, например, Subject Alternative Name. Это расширение позволяет указывать дополнительные имена, для которых сертификат валиден. При этом часть распространённых современных браузеров (в частности, Google Chrome) считают это поле единственным источником имён, соответственно, даже если сертификат содержит корректное имя узла в поле Subject, но не в расширении Subject Alternative Name, он не пройдёт процедуру валидации в браузере.

Ряд расширений в современных сертификатах выполняют служебные функции. Например, расширение Authority Key Identifier позволяет оптимизировать поиск открытого ключа, соответствующего закрытому, которым подписан сертификат. Другое расширение, Certificate Policies, содержит информацию о политиках, в соответствии с которыми был выпущен сертификат. Политики определяют, например, уровень проверки заявителя, который использовался при выпуске: браузеры отличают серверные сертификаты с

расширенной проверкой (EV, Extended Validation) именно по политикам в Certificate Policies.

Можно выделить несколько расширений, которые наиболее важны, так как прямо определяют критические свойства сертификата и открытого ключа, связанного с ним:

1. Basic Constraints

Это расширение задаёт ограничения по использованию данного сертификата. Наиболее важная из его ролей - определение сертификатов, являющихся сертификатами УЦ, то есть, таких сертификатов, открытые ключи из которых могут использоваться для удостоверения других сертификатов.

2. Key Usage

Определяет допустимое использование пары ключей, открытая часть которой указана в сертификате. Типичных сценариев использования ключей два:

- генерация электронной подписи (Signing) и
- шифрование другого ключа (Key Encipherment).

Второй сценарий применим только для RSA и используется при установлении TLS-соединения.

3. Extended Key Usage (некритическое расширение)

Определяет цели, для которых может использоваться открытый ключ из сертификата. Это поле не переопределяет Basic Constraints или Key Usage, а лишь дополняет их (в случае с Key Usage - значения расширений не должны противоречить друг другу). Значение расширения относится к базовым операциям. Например, возможны такие значения: аутентификация сервера, аутентификация клиента, подписывание программного кода и др.

ИНИЦИАТИВА CERTIFICATE TRANSPARENCY

В рамках инициативы Certificate Transparency (CT) ведутся открытые логи сертификатов, выпущенных УЦ. В логи сертификаты добавляются как самими удостоверяющими центрами, так и всеми желающими - это позволяет обнаруживать сертификаты, выпущенные УЦ с нарушением правил и требований; в частности, администраторы доменных зон могут просматривать логи CT с целью обнаружения сертификатов, выпущенных для имён в их зонах без их ведома. Логи сертификатов представляют собой базу данных специального формата, снабжённую криптографически защищённой структурой, что позволяет третьей стороне проверить целостность, подлинность и непротиворечивость данных. Логи могут вести все желающие, однако для включения логов в список известных браузерам требуется, чтобы оператор лога выполнил ряд

достаточно жёстких требований. В 2017 году действует около 20 сервисов логов, часть из них поддерживается Google, большинство других - различными УЦ. Поддержка CT встроена в распространённые браузеры (Chromium/Chrome и базирующиеся на этой ветке браузеры.).

С инициативой CT связано специальное расширение сертификатов: CT Precertificate SCTs, где SCT обозначает Signed Certificate Timestamp. SCT - содержит подписанный электронной подписью «тикет» с отпечатком времени, подтверждающий, что сведения о сертификате были переданы в тот или иной лог CT. Включение данного расширения позволяет TLS-узлу простым методом передать сведения CT подключающемуся клиенту на стадии установления соединения. Это требуется для того, чтобы клиент мог проверить наличие сертификата в логе, а также убедиться, что параметры из лога соответствуют внутренним политикам и именам в предъявленном сертификате. Под «внутренними политиками» здесь имеются в виду, в частности, политики валидации сертификатов браузерами. Например, браузеры могут требовать наличия записи в логе CT для всех EV-сертификатов (с расширенной проверкой).

РЕЗУЛЬТАТЫ: РАСШИРЕНИЯ В ИССЛЕДОВАННЫХ СЕРТИФИКАТАХ

Общие показатели:

Период опроса: июнь 2017

Показатель	**Число**
Всего уникальных TLS-узлов, по IP-адресам	184 930
Всего уникальных TLS-сертификатов	421 236
Всего уникальных валидных TLS-сертификатов (включая промежуточные)	330 944
Всего уникальных валидных серверных TLS-сертификатов	330 629
Всего уникальных валидных серверных TLS-сертификатов для имён .RU (все уровни)	296 119

Повсеместно используется расширение SAN (Subject Alternative Name): 330628 валидных серверных сертификатов. Единственный найденный валидный сертификат без SAN выдан VeriSign для имени LexusMasterClass.ru (Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Secure Server CA - G3).

Ограничения по использованию Basic Constraints (BC)

Основные количественные показатели распространённости расширения BC приведены в таблице 1, из которой видно, что сертификаты без данного расширения практически не встречаются - это соответствует его значению для процедур валидации.

Уникальные валидные сертификаты	**Всего, число**	**Для имен в домене .RU, число**

Серверные сертификаты с BC	330 598	296 109
Серверные сертификаты без BC	31	10

Таблица 1. Статистика Basic Constraints

Немногочисленные серверные сертификаты, выпущенные без расширения BC (см. табл.1.), относятся к корпоративным и пользовательским сервисам корпорации Microsoft (например: сертификат узла outlook.live.com, подписан промежуточным УЦ Microsoft), а также к некоторым банкам, финансовым структурам и другим крупным организациям (пример: компания E.ON - eon.com).

Для валидных серверных сертификатов единственное (успешно распознанное) значение, встречающееся в расширении BC, это флаг, который обозначает, что сертификат не является сертификатом УЦ: *CA:FALSE*.

Для промежуточных и корневых сертификатов (в ответах серверов), соответственно, *CA:TRUE* - то есть, сертификат является сертификатом УЦ. При этом во многих случаях, для сертификатов УЦ, указан параметр Pathlen - этот параметр ограничивает максимальное число промежуточных сертификатов в выстраиваемой цепочке доверия, содержащей данный сертификат (который, при этом, не подсчитывается). Встреченные значения Pathlen:

CA:TRUE, pathlen:2
CA:TRUE, pathlen:0
CA:TRUE, pathlen:1
CA:TRUE, pathlen:12
CA:TRUE, pathlen:5
CA:TRUE, pathlen:4
CA:TRUE, pathlen:3

Значение Pathlen 12 относится к корневому сертификату УЦ «O = AC Camerfirma S.A/CN = Chambers of Commerce Root - 2008».

Допустимое использование ключа Key Usage (KU)

Уникальные валидные сертификаты	**Всего, число**	**Для имен в домене .RU, число**
Серверные сертификаты с KU	330 611	296 113
Серверные сертификаты без KU	18	6

Таблица 2. Статистика Key Usage

Отсутствие KU - также большая редкость: см. Таблицу 2 - все сертификаты без расширения относятся к сервисам Google, и выпущены собственным УЦ соответствующей корпорации («CN=Google Internet Authority G2»).

Варианты значений признаков расширения KU (в терминах OpenSSL, предназначение - соответствует названию), обнаруженные в валидных серверных сертификатах; числовой показатель - количество сертификатов с указанной конфигурацией значений:

Digital Signature, Key Encipherment - 288293
Digital Signature - 42222
Digital Signature, Key Encipherment, Key Agreement - 74
Digital Signature, Key Encipherment, Data Encipherment - 19
Digital Signature, Key Encipherment, Data Encipherment, Key Agreement - 1
Digital Signature, Key Agreement - 1
Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment - 1

Критический набор, необходимый для протокола TLS, - Digital Signature, Key Encipherment (может отсутствовать) - соответствует основной массе сертификатов.

Единственный сертификат с экзотическим «полным» набором флагов Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment выпущен УЦ «/O=Deutsches Zentrum fuer Luft- und Raumfahrt e.V. (DLR)/CN=DLR CA - G02», соответствует имени www.pt-it.de, и наблюдался на веб-узле под именем eu-russia-yearofscience.ru (с несколькими синонимами, для всех сертификат не валиден).

Дополнительное расширение Extended Key Usage (EKU)

Данное расширение (см. Таблицу 3) имеет высокую важность, так как определяет возможные пути построения цепочек доверия, в которые входит ключ, указанный в сертификате. Валидных серверных сертификатов без EKU - не обнаружено.

Уникальные валидные сертификаты	**Всего, число**	**Для имен в домене .RU, число**
Серверные сертификаты с EKU	330 629	296 119
Серверные сертификаты без EKU	0	0

Таблица 3. Статистика Extended Key Usage

Варианты значений признаков расширения EKU (в терминах OpenSSL, предназначение соответствует названию), обнаруженные в валидных серверных сертификатах (числовой показатель - количество сертификатов с указанной конфигурацией значений):

TLS Web Server Authentication, TLS Web Client Authentication - 326087
TLS Web Client Authentication, TLS Web Server Authentication - 4467
TLS Web Server Authentication - 43
TLS Web Server Authentication, TLS Web Client Authentication, Microsoft Server Gated Crypto, Netscape Server Gated Crypto - 24
TLS Web Client Authentication, E-mail Protection - 4
TLS Web Server Authentication, TLS Web Client Authentication, 2.16.840.1.113741.1.2.3 - 4

Идентификатор OID 2.16.840.1.113741.1.2.3 - соответствует некоторым схемам аутентификации сервисов удалённого управления, используемым в корпоративном окружении, в частности, Intel vPro AMT и др. Является устаревшим.

Microsoft Server Gated Crypto, Netscape Server Gated Crypto - устаревшие флаги, обозначающие возможность использования ключа сертификата для «экспортных» вариантов внедрения SSL, с «контролируемым повышением» криптографической стойкости (Server Gated Cryptography - SGC), которое было доступно для финансовых учреждений.

Число валидных серверных сертификатов, у которых присутствуют оба расширения: 330611.

Исследование расширений Certificate Transparency (CT)

При исследовании данных расширений (CT) использовалась выборка всех серверных сертификатов (строка «Всего» в Таблице 4), полученных с узлов, адресуемых доменами .RU, .SU, .РФ, то есть - без выделения сертификатов, относящихся к данным зонам по именам. Данные внутри расширения - не валидировались (валидировался только сам сертификат).

Уникальные валидные сертификаты	**Всего, число**	**Для имен в домене .RU, число**
Серверные сертификаты с CT	42 049	37 665
Серверные сертификаты без CT	288 580	258 454

Таблица 4. Распространённость CT-расширений

Всего уникальных валидных серверных сертификатов, с обнаруженными расширениями CT: 42049. Расширение "CT Precertificate SCT" представляет собой подписанный ответ лога CT, содержащий метку времени и подтверждающий, что данный сертификат был успешно отправлен в тот или иной лог. Идентификатор лога, представляющий собой отпечаток открытого ключа, включается в состав расширения. Возможно включение нескольких ответов SCT в сертификат. Большинство обнаруженных сертификатов с CT содержат отметки нескольких логов.

В таблице ниже отражено распределение сертификатов по числу логов, на которые они ссылаются.

Число логов в CT	**Число сертификатов**
5	23 812
2	13 654
4	2 795
3	1 787
1	1

Таблица 5. Распределение сертификатов по числу логов

Наиболее часто встречающиеся в сертификатах логи принадлежат Google и Symantec. Рейтинг логов, обнаруженных в сертификатах, по числу уникальных сертификатов отображен в таблице 6.

Название лога	**Число сертификатов**
Symantec log	38 965
Google 'Pilot' log	38 403
Google 'Rocketeer' log	29 101
DigiCert Log Server	24 489
Google 'Skydiver' log	18 866
Google 'Aviator' log	9 755
StartCom log	1 728
WoSign log	861
Symantec 'Vega' log	705
Certly.IO log	14
Venafi log	13
Izenpe log	8
WoSign CT log #1	1
Symantec Deneb	1

Таблица 6. Рейтинг логов по числу сертификатов

В обнаруженных расширениях используется только версия v.1(0).

Практически все распространённые УЦ встречаются в различных логах. Распределение УЦ по нескольким крупнейшим логам приведено в Приложении 1.

ВЫВОД

В результате регулярного обхода узлов, адресуемых доменами российских зон, накоплено большое число сертификатов, содержащих расширения X509. В рамках данного исследования построена и проанализирована статистика по ключевым (с точки зрения прикладного применения протокола TLS) X509-расширениям и значениям параметров этих расширений.

Массовых аномалий не выявлено. Картина на TLS-узлах Рунета соответствует общим тенденциям и по составу типов сертификатов, и по значениям параметров. В Рунете распространены сертификаты, включающие тикеты (метки времени) новой инициативы по контролю за деятельностью удостоверяющих центров - Certificate Transparency.

Результаты свидетельствуют о стабильном и предсказуемом, на настоящий момент, развитии технологий TLS для HTTPS в Рунете.

Приложение 1. Распределение УЦ по логам

Обозначения и формат. Вверху приведено имя лога. Number of certs - число сертификатов, в которых используется SCT данного лога; Number of dif. CAs - число различных УЦ (это значение поля Issuer сертификата); CA-List - список УЦ.

Symantec log:
Number of certs: 38965
Number of dif. CAs: 29
CA-List:
[/C=US/O=thawte, Inc./CN=thawte SHA256 SSL CA]
[/C=US/O=thawte, Inc./CN=thawte EV SSL CA - G3]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA - G3]
[/C=US/O=GeoTrust Inc./CN=GeoTrust EV SSL CA - G4]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA - G2]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL CA - G3]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SHA256 SSL CA]
[/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2014 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1M]
[/C=US/O=thawte, Inc./CN=thawte Extended Validation SHA256 SSL CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL SHA256 CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/OU=Domain Validated SSL/CN=Symantec Basic DV SSL CA - G2]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server SHA256 SSL CA]
[/C=NL/O=Trust Provider B.V./OU=Domain Validated SSL/CN=Trust Provider B.V. DV SSL CA - G2]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL SHA256 CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Extended Validation SHA256 SSL CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2]
[/C=CN/O=WoSign CA Limited/CN=WoSign CA Free SSL Certificate G2]
[/C=CN/O=TrustAsia Technologies, Inc./OU=Symantec Trust Network/OU=Domain Validated SSL/CN=TrustAsia DV SSL CA - G5]
[/C=US/O=GeoTrust Inc./CN=GeoTrust Extended Validation SHA256 SSL CA]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G3]
[/C=US/O=GeoTrust, Inc./OU=Domain Validated SSL/CN=Secure Site Starter DV SSL CA - G2]
[/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Extended Validation CA SHA2]

[/C=US/O=thawte, Inc./CN=thawte SSL CA - G2]

Google 'Pilot' log:
Number of certs: 38403
Number of dif. CAs: 44
CA-List:
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SHA256 SSL CA]
[/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2014 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1M]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 4 EV Server CA]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA]
[/C=CN/O=WoSign CA Limited/CN=WoSign Class 1 DV Server CA G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3]
[/C=CN/O=WoSign CA Limited/CN=CA \xE6\xB2\x83\xE9\x80\x9A\xE5\x85\x8D\xE8\xB4\xB9SSL\xE8\xAF\x81\xE4\xB9\xA6 G2]
[/C=US/O=GeoTrust Inc./CN=GeoTrust EV SSL CA - G4]
[/C=US/O=thawte, Inc./CN=thawte EV SSL CA - G3]
[/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL High Assurance CA 3]
[/C=US/O=SSL.com/OU=Controlled by COMODO exclusively for SSL.com/OU=www.ssl.com/CN=SSL.com Premium EV CA]
[/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Extended Validation CA SHA2]
[/C=US/O=thawte, Inc./CN=thawte SSL CA - G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA 2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2]
[/C=US/O=GeoTrust, Inc./OU=Domain Validated SSL/CN=Secure Site Starter DV SSL CA - G2]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=UbiquiTLS\xE2\x84\xA2 DV RSA Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust Extended Validation SHA256 SSL CA]
[/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 2 IV Server CA]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL SHA256 CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Extended Validation SHA256 SSL CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/OU=Domain Validated SSL/CN=Symantec Basic DV SSL CA - G2]

[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server SHA256 SSL CA]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3]
[/C=US/O=thawte, Inc./CN=thawte Extended Validation SHA256 SSL CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL SHA256 CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 1 DV Server CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL CA - G3]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA - G3]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA - G2]
[/C=US/O=thawte, Inc./CN=thawte SHA256 SSL CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 3 OV Server CA]
[/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G3]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Extended Validation Server CA]
[/C=CN/O=WoSign CA Limited/CN=WoSign CA Free SSL Certificate G2]
[/C=NL/O=Trust Provider B.V./OU=Domain Validated SSL/CN=Trust Provider B.V. DV SSL CA - G2]

Google 'Rocketeer' log:
Number of certs: 29101
Number of dif. CAs: 37
CA-List:
[/C=US/O=thawte, Inc./CN=thawte Extended Validation SHA256 SSL CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL SHA256 CA]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA - G2]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA - G3]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL CA - G3]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 1 DV Server CA]
[/C=US/O=thawte, Inc./CN=thawte SHA256 SSL CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G3]
[/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 3 OV Server CA]
[/C=CN/O=WoSign CA Limited/CN=WoSign CA Free SSL Certificate G2]
[/C=NL/O=Trust Provider B.V./OU=Domain Validated SSL/CN=Trust Provider B.V. DV SSL CA - G2]

[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 4 EV Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SHA256 SSL CA]
[/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2014 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1M]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4]
[/C=US/O=GeoTrust Inc./CN=GeoTrust EV SSL CA - G4]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3]
[/C=US/O=thawte, Inc./CN=thawte EV SSL CA - G3]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2]
[/C=US/O=thawte, Inc./CN=thawte SSL CA - G2]
[/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Extended Validation CA SHA2]
[/C=US/O=GeoTrust Inc./CN=GeoTrust Extended Validation SHA256 SSL CA]
[/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA]
[/C=CN/O=TrustAsia Technologies, Inc./OU=Symantec Trust Network/OU=Domain Validated SSL/CN=TrustAsia DV SSL CA - G5]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Extended Validation SHA256 SSL CA]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL SHA256 CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 2 IV Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server SHA256 SSL CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/OU=Domain Validated SSL/CN=Symantec Basic DV SSL CA - G2]

DigiCert Log Server:
Number of certs: 24489
Number of dif. CAs: 19
CA-List:
[/C=US/O=thawte, Inc./CN=thawte EV SSL CA - G3]
[/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2014 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1M]
[/C=US/ST=Illinois/L=Chicago/O=Trustwave Holdings, Inc./CN=Trustwave Extended Validation SHA256 CA, Level 1/emailAddress=ca@trustwave.com]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA]

[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA - G3]
[/C=US/O=GeoTrust Inc./CN=GeoTrust EV SSL CA - G4]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Extended Validation Secure Server CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA 2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G3]
[/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL High Assurance CA 3]
[/C=US/O=SSL.com/OU=Controlled by COMODO exclusively for SSL.com/OU=www.ssl.com/CN=SSL.com Premium EV CA]
[/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=UbiquiTLS\xE2\x84\xA2 DV RSA Server CA]
[/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA]

Google 'Skydiver' log:
Number of certs: 18866
Number of dif. CAs: 19
CA-List:
[/C=US/O=thawte, Inc./CN=thawte SHA256 SSL CA]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA - G2]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL CA - G3]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 1 DV Server CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/OU=Domain Validated SSL/CN=Symantec Basic DV SSL CA - G2]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL SHA256 CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 2 IV Server CA]
[/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA]

[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G3]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2]
[/C=US/O=thawte, Inc./CN=thawte SSL CA - G2]
[/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 3 OV Server CA]

Google 'Aviator' log:
Number of certs: 9755
Number of dif. CAs: 41
CA-List:
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 4 EV Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SHA256 SSL CA]
[/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2014 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1M]
[/C=US/ST=Illinois/L=Chicago/O=Trustwave Holdings, Inc./CN=Trustwave Extended Validation SHA256 CA, Level 1/emailAddress=ca@trustwave.com]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4]
[/C=US/O=GeoTrust Inc./CN=GeoTrust EV SSL CA - G4]
[/C=CN/O=WoSign CA Limited/CN=CA \xE6\xB2\x83\xE9\x80\x9A\xE5\x85\x8D\xE8\xB4\xB9SSL\xE8\xAF\x81\xE4\xB9\xA6 G2]
[/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3]
[/C=CN/O=WoSign CA Limited/CN=WoSign Class 1 DV Server CA G2]
[/C=US/O=thawte, Inc./CN=thawte EV SSL CA - G3]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA 2]
[/C=US/O=SSL.com/OU=Controlled by COMODO exclusively for SSL.com/OU=www.ssl.com/CN=SSL.com Premium EV CA]
[/C=US/O=thawte, Inc./CN=thawte SSL CA - G2]
[/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL High Assurance CA 3]
[/C=US/O=GeoTrust Inc./CN=GeoTrust Extended Validation SHA256 SSL CA]
[/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2]
[/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2]
[/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL SHA256 CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 2 IV Server CA]
[/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3]

[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/OU=Domain Validated SSL/CN=Symantec Basic DV SSL CA - G2]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server SHA256 SSL CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL SHA256 CA]
[/C=US/O=thawte, Inc./CN=thawte Extended Validation SHA256 SSL CA]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA]
[/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA - G2]
[/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA - G3]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 1 DV Server CA]
[/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL CA - G3]
[/C=US/O=thawte, Inc./CN=thawte SHA256 SSL CA]
[/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 3 OV Server CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Extended Validation Server CA]
[/C=CN/O=WoSign CA Limited/CN=WoSign CA Free SSL Certificate G2]
[/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Extended Validation Secure Server CA]
[/C=NL/O=Trust Provider B.V./OU=Domain Validated SSL/CN=Trust Provider B.V. DV SSL CA - G2]

StartCom log:
Number of certs: 1728
Number of dif. CAs: 3
CA-List:
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 2 IV Server CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 3 OV Server CA]
[/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 1 DV Server CA]

Соответственно, сертификаты конкретных УЦ встречаются в различных логах CT. Рейтинг УЦ (Subject CN) по числу различных логов, которые указаны в сертификатах (SCT):

/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 3 OV Server CA::8
/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 1 DV Server CA::7
/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 2 IV Server CA::7
/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA - G3::6
/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA::6
/C=US/O=GeoTrust Inc./CN=RapidSSL SHA256 CA - G2::6

/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL CA - G3::6
/C=US/O=thawte, Inc./CN=thawte SHA256 SSL CA::6
/C=US/O=GeoTrust Inc./CN=GeoTrust EV SSL CA - G4::6
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA::6
/C=US/O=GeoTrust Inc./CN=GeoTrust SHA256 SSL CA::6
/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=(c) 2014 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1M::6
/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Class 4 EV Server CA::6
/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server CA - G4::6
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server CA::6
/C=US/O=thawte, Inc./CN=thawte EV SSL CA - G3::6
/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2::6
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G2::6
/C=US/O=thawte, Inc./CN=thawte SSL CA - G2::6
/C=US/O=Symantec Corporation/OU=Symantec Trust Network/OU=Domain Validated SSL/CN=Symantec Basic DV SSL CA - G2::6
/C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3::6
/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL SHA256 CA::6
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G2::6
/C=US/O=thawte, Inc./CN=thawte Extended Validation SHA256 SSL CA::5
/C=US/O=GeoTrust Inc./OU=Domain Validated SSL/CN=GeoTrust DV SSL SHA256 CA::5
/C=CN/O=WoSign CA Limited/CN=WoSign CA Free SSL Certificate G2::5
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Domain Validation CA - SHA256 - G3::5
/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com,
Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2::5
/C=NL/O=Trust Provider B.V./OU=Domain Validated SSL/CN=Trust Provider B.V. DV SSL CA - G2::5
/C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3::5
/C=US/O=GeoTrust Inc./CN=GeoTrust Extended Validation SHA256 SSL CA::5
/C=US/O=DigiCert Inc/CN=DigiCert SHA2 Secure Server CA::5
/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Secure Server SHA256 SSL CA::5
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA::5
/C=PL/O=Unizeto Technologies S.A./OU=Certum Certification Authority/CN=Certum Extended Validation CA SHA2::4
/C=IL/O=StartCom Ltd./OU=StartCom Certification Authority/CN=StartCom Extended Validation Server CA::3
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Extended Validation Secure Server CA 2::3
/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL High Assurance CA 3::3
/C=US/O=SSL.com/OU=Controlled by COMODO exclusively for SSL.com/OU=www.ssl.com/CN=SSL.com Premium EV CA::3
/C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 Extended Validation SHA256 SSL CA::3
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO ECC Extended Validation Secure Server CA::2
/C=CN/O=WoSign CA Limited/CN=WoSign Class 1 DV Server CA G2::2

/C=CN/O=WoSign CA Limited/CN=CA \xE6\xB2\x83\xE9\x80\x9A\xE5\x85\x8D\xE8\xB4\xB9SSL\xE8\xAF\x81\xE4\xB9\xA6 G2::2
/C=US/ST=Illinois/L=Chicago/O=Trustwave Holdings, Inc./CN=Trustwave Extended Validation SHA256 CA, Level 1/emailAddress=ca@trustwave.com::2
/C=CN/O=TrustAsia Technologies, Inc./OU=Symantec Trust Network/OU=Domain Validated SSL/CN=TrustAsia DV SSL CA - G5::2
/C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=UbiquiTLS\xE2\x84\xA2 DV RSA Server CA::2
/C=US/O=GeoTrust, Inc./OU=Domain Validated SSL/CN=Secure Site Starter DV SSL CA - G2::2