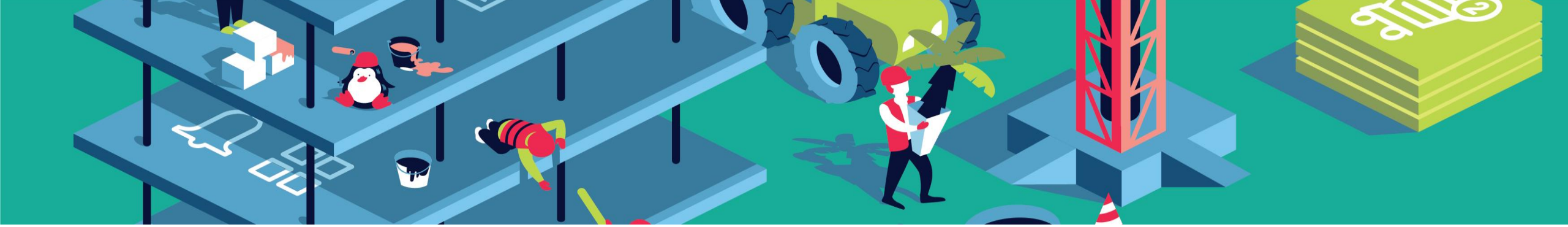
hoster.by

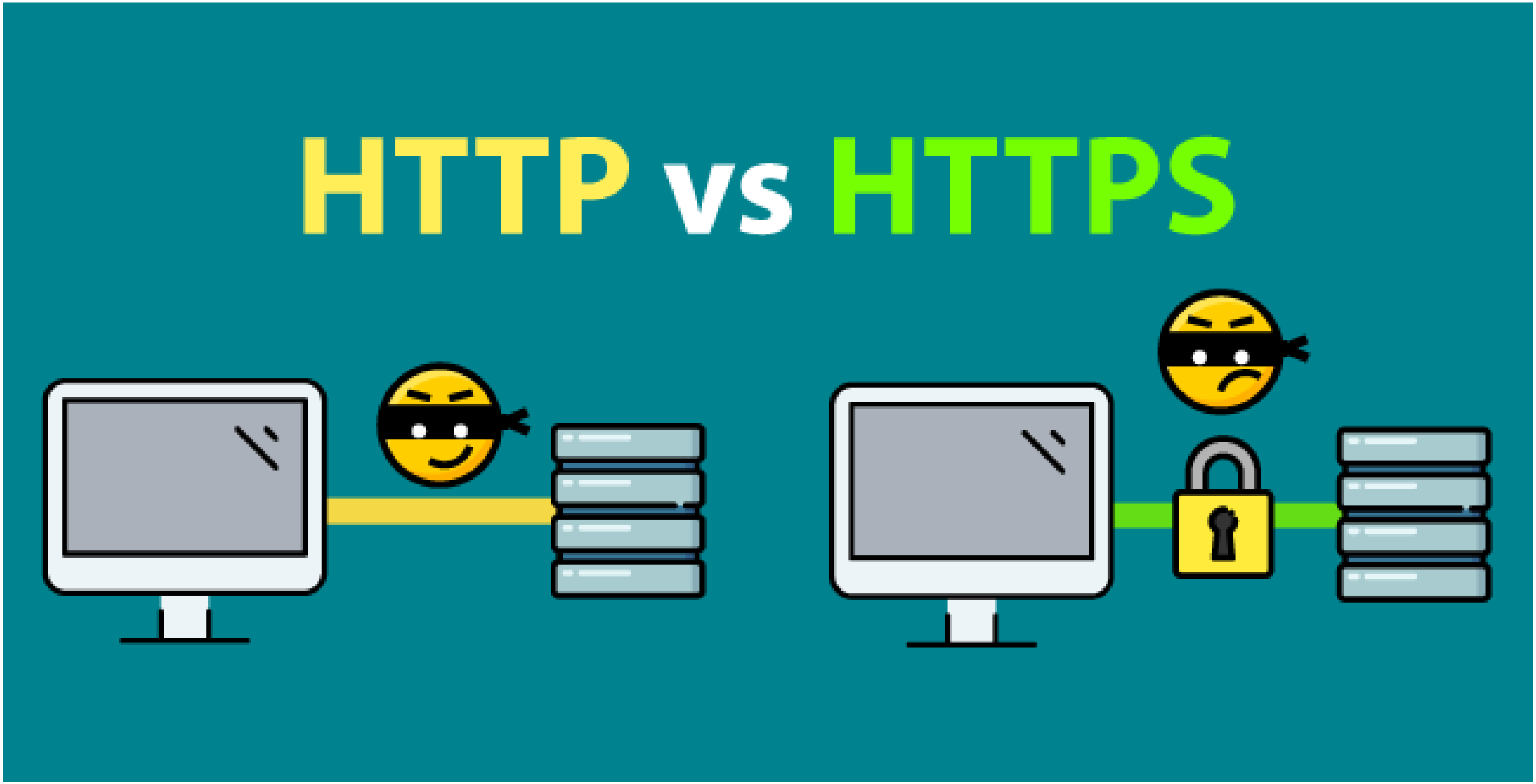
Все, что вам нужно знать об SSL-сертификатах

Артем Стецко
руководитель отдела по работе с клиентами


hoster.by
HTTPS
Google
SSL
СЕРТИФИКАТЫ
Повысить уровень доверия поисковиков и защитить личные данные пользователей



SSL (Secure Socket Layer) — это интернет технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером.

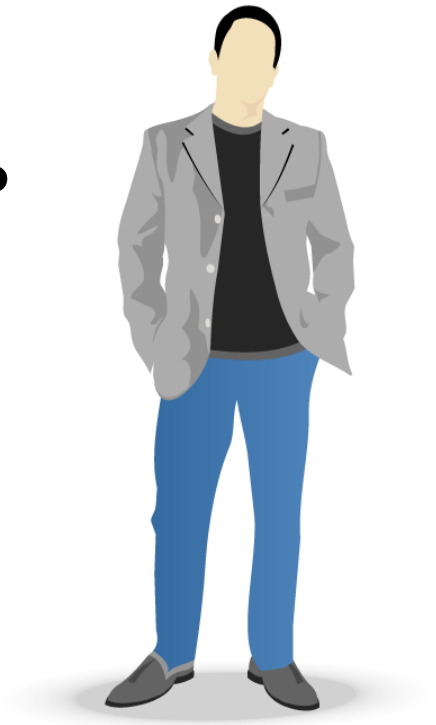

HTTP vs HTTPS

Как получить SSL сертификат?

Самоподписной сертификат (self-signed)

Плюсы

- **Можно сгенерировать прямо на веб-сервере**
- **Вы ничего не платите за его создание**



Минусы

- **Браузеры будут выдавать ошибку, с предупреждением, что сайт не проверен.**

Чтобы получить SSL сертификат нужно:

Сформировать специальный запрос (Certificate Signing Request) на выпуск сертификата

Ответить наряд вопросов, для уточнения деталей о вашем домене и вашей компании.

После завершения ваш веб сервер создаст 2 типа криптографических ключей — приватный ключ и публичный ключ.
*Публичный ключ не является секретным и он помещается в запрос CSR.

Пример

CSR Information:
Common Name: hoster.by — доменное имя, которое мы защищаем таким сертификатом
Organization: Reliable Software LLC — название организации, которой принадлежит домен
Organization Unit: IT — подразделение организации
Locality: Minsk — город, где находится офис организации
State: MInsk — область или штат
Country: BY — двухбуквенный код, страны офиса.
Email: info@hoster.by — контактный email технического администратора или службы поддержки

-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwgZkxCzAJBgNVBAYTAlVBMQ0wCwYDVQQIEwRLaWV2MQ0wCwYDVQQHEwRLaWV2MRQwEgYDVQQKEwtIb3N0
QXV0b21hdDEQMA4GA1UECxMHaG9zdGluZzEmMCQGCSqGSIb3DQEJARYXc3VwcG9ydEBob3N0YXV0b21hdC5jb20xHDAaBgNVBA
MTE3d3dy5ob3N0YXV0b21hdC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDTg7iUv/iX+SyZl74GcUVFHjFC5IqlTN
EzWgLWrsSmxGxlGzXkUKidNyXWa0O3ayJHOiv1BSX1l672tTqeHxhGuM6F7l5FTRWUyFHUxSU2Kmci6vR6fw5ccgWOMMNdMg7V5b
MOD8tfI74oBkVE7hV95Ds3c594u7kMLvHR+xui2S3z2JJQEwChmfllojGnSCO/iv64RL9vjZ5B4jAWJwrruIXO5ILTdis41Z1nNIx3bBqkif0H/
G4eO5WF6fFb7etm8M+d8ebkqEztRAVdhXvTGBZ4Mt2DOV/bV4e/ffmQJxffTYEqWg8wb465GdAJcLhhiSaHgqRzrprKns7QSGjdAgMBA
AGgADANBgkqhkiG9w0BAQUFAAOCAQEAuCfJKehyjt7N1IDv44dd+V61MIqlDhna0LCXH1uT7R9H8mdlnuk8yevEcCRIkrnWAlA9GT3Vk
OY3Il4WTGg3wmtq6WAgLkVXQnhIpGDdYAflpAVeMKil8Z46BGIhKQGngL2PjWdhMVLlRTB/01nVSKSEk2jhO8+7yLOY1MoGIvwAEF4CL
1lAjov8U4XGNfQldSWT1o8z9sDeGsGSf5DAXpcccx0gCyk90HFJxhbm/vTxjJgchUFro/0goVpBcredpKxtkwBMuCzeSyDnkQft0eLtZ9b9Q4
+ZNDWsPPKxo/zWHm6Pa/4F4o2QKvPCPx9x4fm+/xHqkhkR79LxJ+EHzQ==
-----END CERTIFICATE REQUEST-----

Что такое центр сертификации (CA)?

Это организация, которая обладает правом выдачи цифровых сертификатов.

Она производит проверку данных, содержащихся в CSR, перед выдачей сертификата.

В самых простых сертификатах проверяется только соответствие доменного имени, в самых дорогих производится целый ряд проверок самой организации, которая запрашивает сертификат.

Типы сертификатов по типу валидации

Сертификаты, которые подтверждают только доменное имя (Domain Validation (DV)

Сертификаты, которые подтверждают домен и организацию (Organization Validation — OV).

Сертификаты, с расширенной проверкой (Extendet Validation — EV).

Типы SSL сертификатов по своим свойствам

- Обычные SSL сертификаты
- Wildcard сертификаты
- SAN сертификаты
- EV сертификаты
- Сертификаты с поддержкой IDN

hoster.by

e-mail: info@hoster.by
тел.: +375 (17) 239 57 02