

КАК ПОСТРОИТЬ ГЛОБАЛЬНОЕ ДОВЕРИЕ В СЕТИ ИНТЕРНЕТ

ДОВЕРЕННЫЙ ПОЛЬЗОВАТЕЛЬ
ДОВЕРЕННЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР



Andrzej Bendig-Wielowiejski
PKI-FORUM 2011
21-09-2011г. Санкт-Петербург

СОДЕРЖАНИЕ



-
- 1. ДОВЕРИЕ В СЕТИ – ОБЩИЕ ИНФОРМАЦИИ**
 - 2. ДОВЕРИЕ - ВРЕМЯ И ЗАТРАТЫ**
 - 3. БЕЗОПАСНОСТЬ И РИСКИ**
-

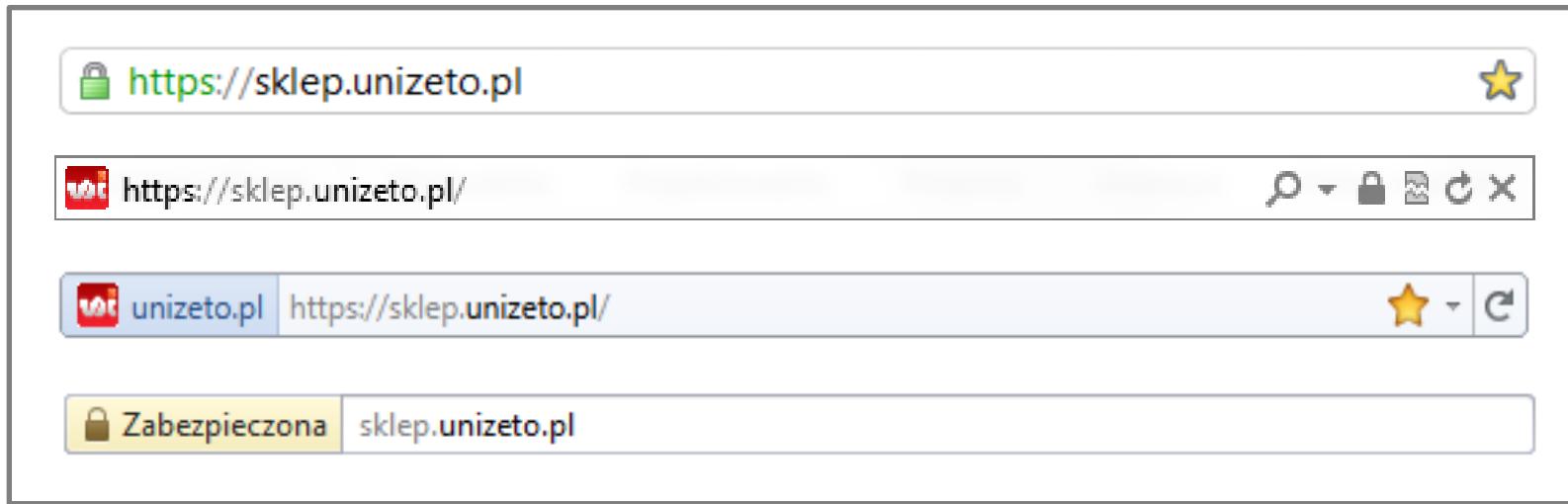
Доверенные сертификационные услуги

предоставляют возможность достоверного удостоверения личности физических и юридических лиц а также е-сервисов в интернет сети в целом мире .

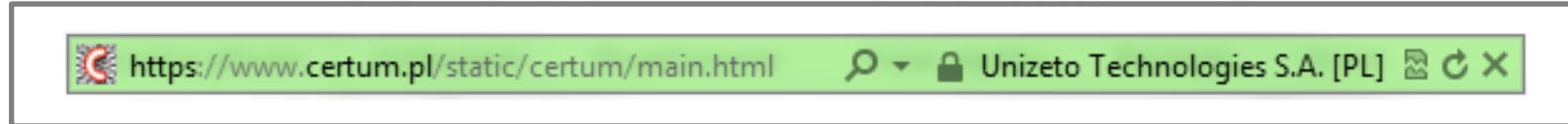
Только сертификаты издаваемые Удостоверяющими Центрами, которые выполняют суровые требования могут получить название глобально доверенных.

ДОВЕРИЕ В СЕТИ PL-EN-RU-...

СТАНДАРТНЫЙ СЕРТИФИКАТ SSL



СЕРТИФИКАТ EV SSL



WebTrust это:

мировой стандарт определяющий множество правил и критерий (хороших практик) в области широко понятой безопасности информации в Интернете. Критерия стандарта WebTrust Certification Authorities и Extended Validation Audit Criteria, установлены организацией AICPA/CICA (The American Institute of Certified Public Accountants/ Canadian Institute of Chartered Accountants) в 1995 году и далее развиваются. Субъект (УЦ) который прошел положительный аудит на соответствие с этим стандартом получает возможность записи в доверенных списках удостоверяющих центров во всем мире, например, во всех распространенных интернет-браузерах, платформах интернет услуг и программном обеспечении.

ДОВЕРИЕ В СЕТИ

WebTrust это:

Безопасность

Доверие во всем мире

Достоверность

Аудит WebTrust охватывает 6 основных областей

1. Security (безопасность)
2. Privacy (защита персональных данных)
3. Business Practices/Transaction Integrity
(бизнес практики/ интегральность транзакций)
4. Availability (доступность)
5. Confidentiality (конфиденциальность)
6. Non-Reputation (неопровергимость)

ДОВЕРИЕ - ВРЕМЯ И ЗАТРАТЫ

Этап 1

Предварительный анализ – УЦ совместно с аудитором определяет свои требования и анализирует требования стандарта

2 – 3
месяца

Этап 2

Функционирование УЦ - как минимум

2
месяца

Этап 3

Пре-Аудит (перед сертификацией) – Аудитор проводит предварительный аудит системы, определяет контрольные механизмы, тестирует их соответствие и определяет отклонения

1,5 – 2
месяца

Этап 4

Устранение определенных отклонений – УЦ ликвидирует определенные аудитором отклонения

3 – 8
месяцев

ДОВЕРИЕ - ВРЕМЯ И ЗАТРАТЫ

Этап 5

Функционирование УЦ согласно всем требованиям
WebTrust

2 – 3
месяца

Этап 6

Сертификационный контроль – Аудитор проводит проверки,
подготавливает рапорт вместе с выводами и вносит заявку о
присвоении сертификата соответствия WebTrust

1- 3
месяца

Этап 7

Сертификационный контроль – первый после 6 месяцев,
очередные каждые 12 месяцев; после истечения 12 месяцев
Аудитор выполняет просмотр изменений системы, проверяет
контрольные механизмы и актуализирует рапорт

после 6
месяцев

Этап 8

Контрольные аудиты - длительность

1
месяц

ДОВЕРИЕ - ВРЕМЯ И ЗАТРАТЫ

Время итого :

- 31 – 40 м-цев

Расходы (приблизительно):
до 2 млн EUR

ДОВЕРИЕ - ВРЕМЯ И ЗАТРАТЫ

Время дистрибуции сертификатов Root в самых распространенных браузерах и ОС(в месяцах)

- Internet Explorer/Windows –8-9 ,
- Mac OS X (Apple) – 4-12,
- Java – 4-12 ,
- Mozilla/Firefox - 12-15 официально, фактически 18-21,
- Windows Mobile/Nokia – практически нет возможности для новых УЦ

**Время не включает времени дистрибуции новых версий браузеров
среди пользователей – в среднем очередные 2-6 м-цев**

ДОВЕРИЕ - ВРЕМЯ И ЗАТРАТЫ

**Общее время ожидание на распространение
Rootów УЦ в интернет-браузерах:**
6-27 месяцев

**Помимо наличия сертификата соответствия WebTrust
сертификаты УЦ в дальнейшем, еще длительное время
не видны как доверенные**

БЕЗОПАСНОСТЬ И РИСКИ

С 2010 года хакер
с псевдонимом ComodoHacker
скорее всего проживающий
в Иране «тестирует»
безопасность УЦ во всем мире

Его атаки коснулись
таких УЦ как

- Comodo (03-2011)
- Startcom (06-2011)
- DigiNotar (07-2011)
- GlobalSign (09-2011)

БЕЗОПАСНОСТЬ И РИСКИ

Случай DigiNotar

- **10.07.2011** – первый неуполномоченный вход в УЦ DigiNotar и издание 283 подделанных сертификатов
- **18-19.07.2011** – очередные 248 подделанных сертификатов
- **29.08.2011** – **обнаружение** подделанного сертификата, изданного для **google.com**, первая **информация с УЦ** о неуполномоченном входе хакером с псевдонимом ComodoHacker , **удаление** Root УЦ DigiNotar со всех распространенных браузеров
- **09.2011** – **сертификаты УЦ DigiNotar**, как и сама фирма теряют доверие во всем мире, **которое строила многие годы !**

Спасибо за внимание

