ТТК БАНКА АД СКОПЈЕ - ЕЛЕКТРОНСКО БАНКАРСТВО

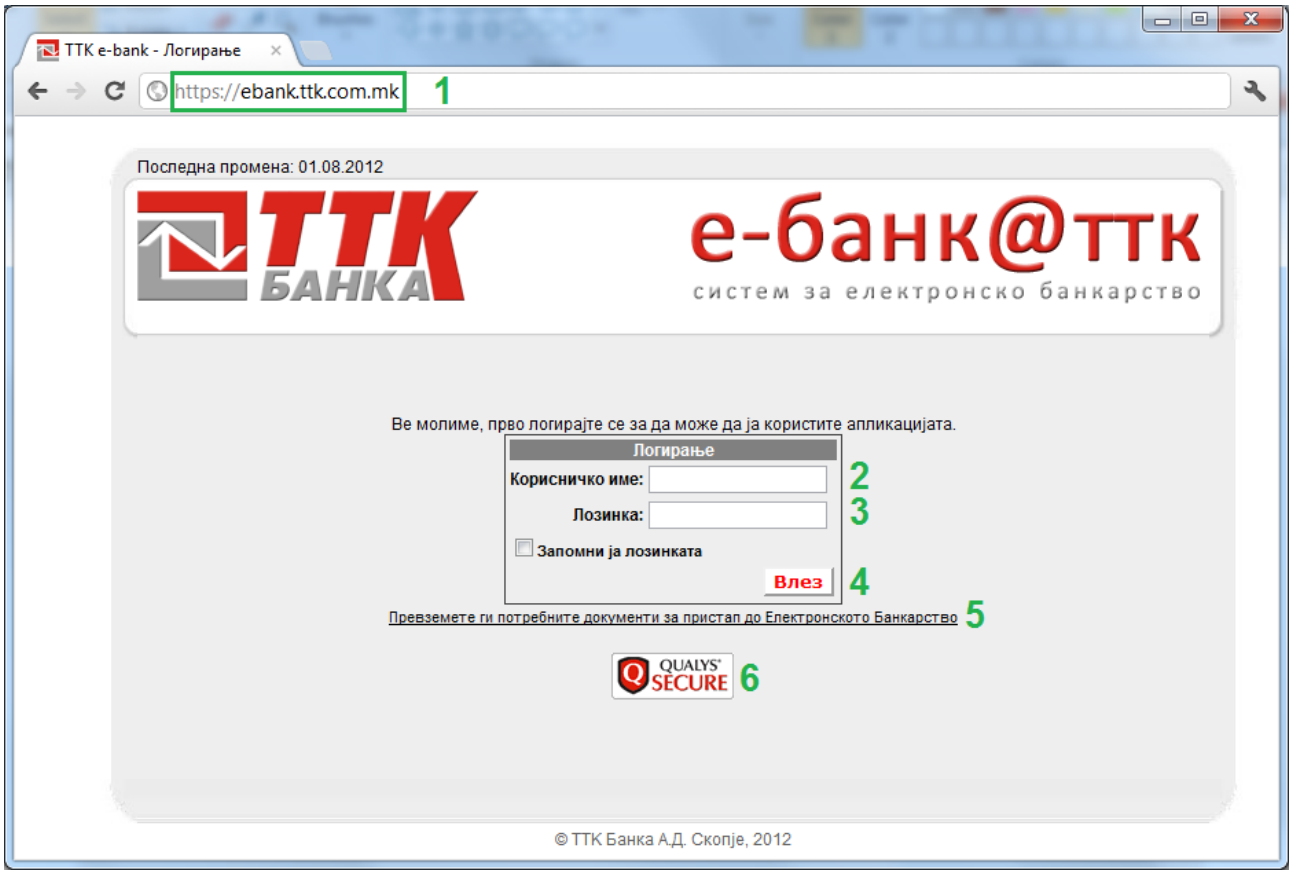
ПРЕПОРАКИ ЗА КЛИЕНТИТЕ ЗА СИГУРНО КОРИСТЕЊЕ НА ЕЛЕКТРОНСКИТЕ БАНКАРСКИ УСЛУГИ

СКОПЈЕ, СЕПТЕМВРИ 2016

СОДРЖИНА

СТРАНА ЗА НАЈАВА НА ЕЛЕКТРОНСКО БАНКАРСТВО

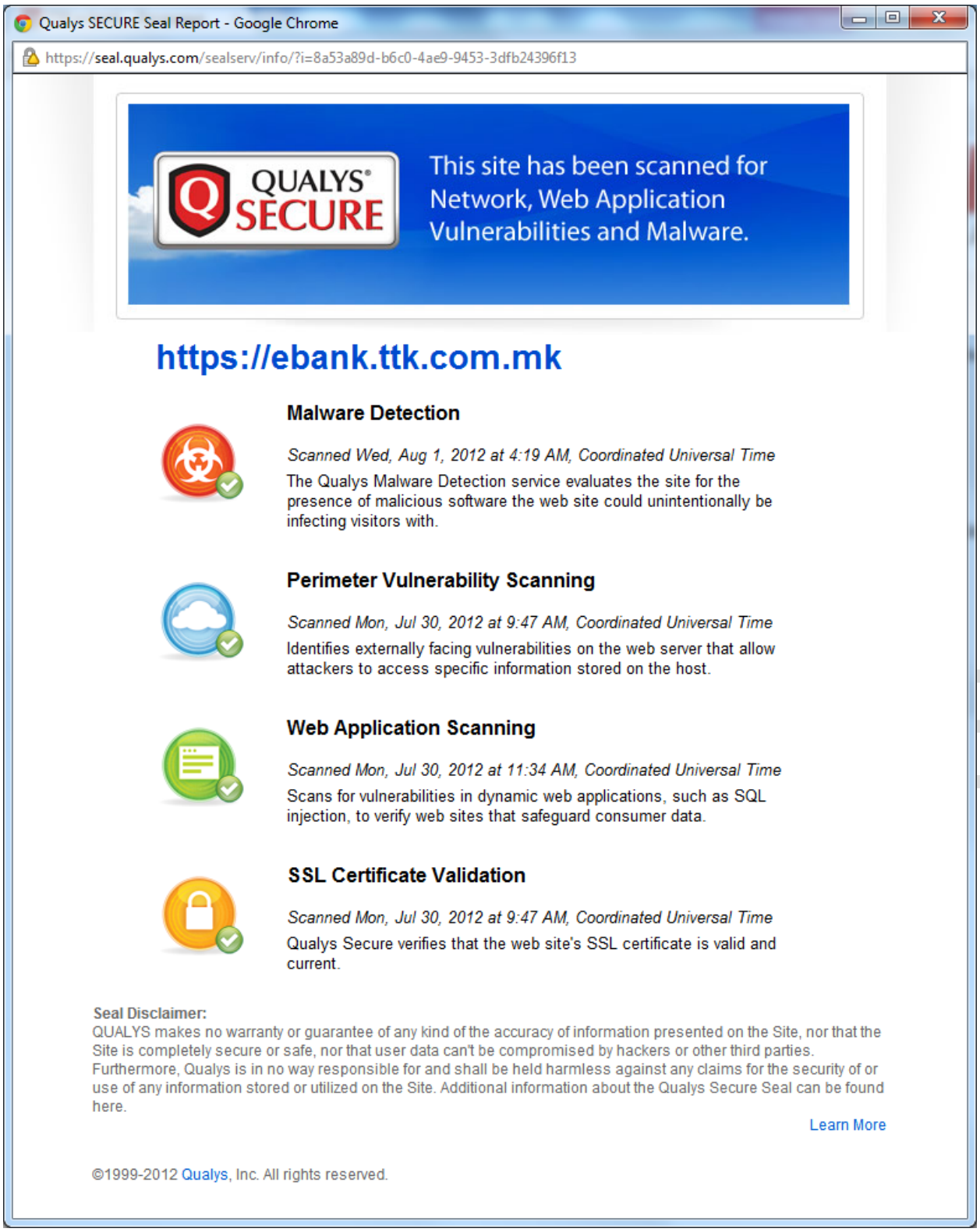
Пристапување до услугите на електронско банкарство на ТТК Банка се врши преку веб пребарувач од веб адресата *https://ebank.ttk.com.mk* **(1)**, по што се појавува почетната страна на електронското банкарство (*Слика 1 Почетна страна на електронско банкарство на ТТК Банка*) каде се внесува корисничкото име **(2)** и лозинката **(3)** добиени од Банката. По внесувањето на корисничкото име и лозинката со кликнување на копчето "Влез" **(4)** се корисникот се логира на системот за електронско банкарство.



Слика 1 Почетна страна на електронско банкарство на ТТК Банка

БЕЗБЕДНОСНИ ПРОВЕРКИ НА ЕЛЕКТРОНСКОТО БАНКАРСТВО

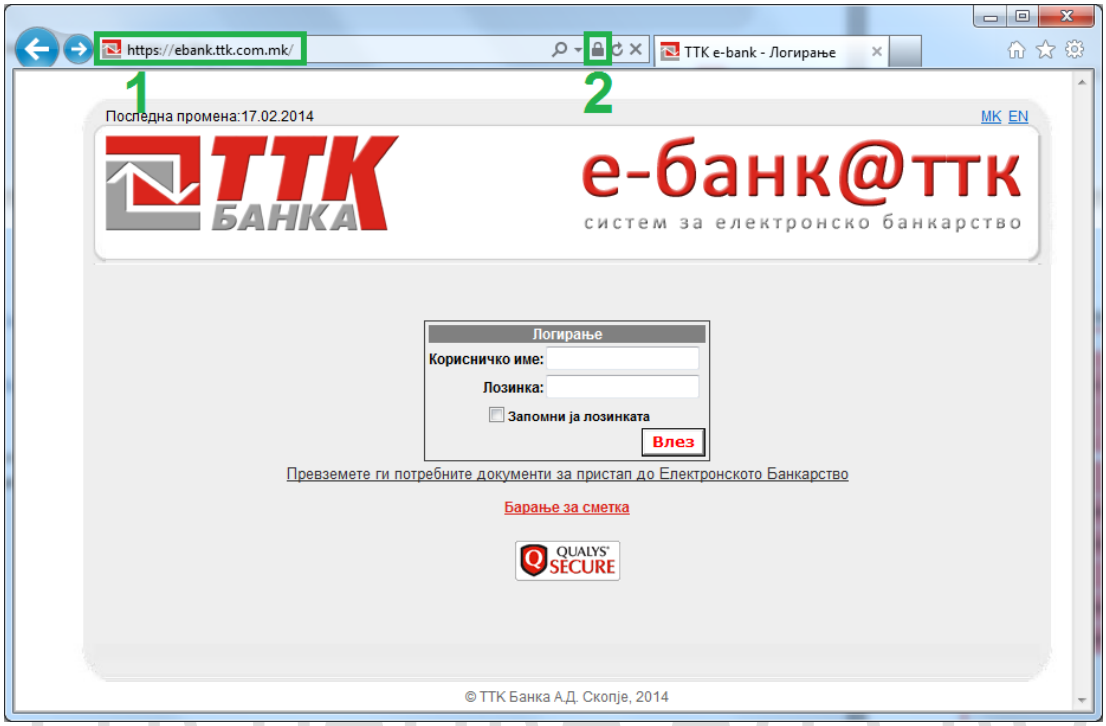
Со кликање на линкот QUALYS® SECURE **(6)** се прикажува извештај за безбедносните проверки кои постојано се вршат на сајтот за електронско банкарство од страна на QUALYS® (*Слика 2 Извештај за безбедносните проверки на сајтот за електронско банкарство*).



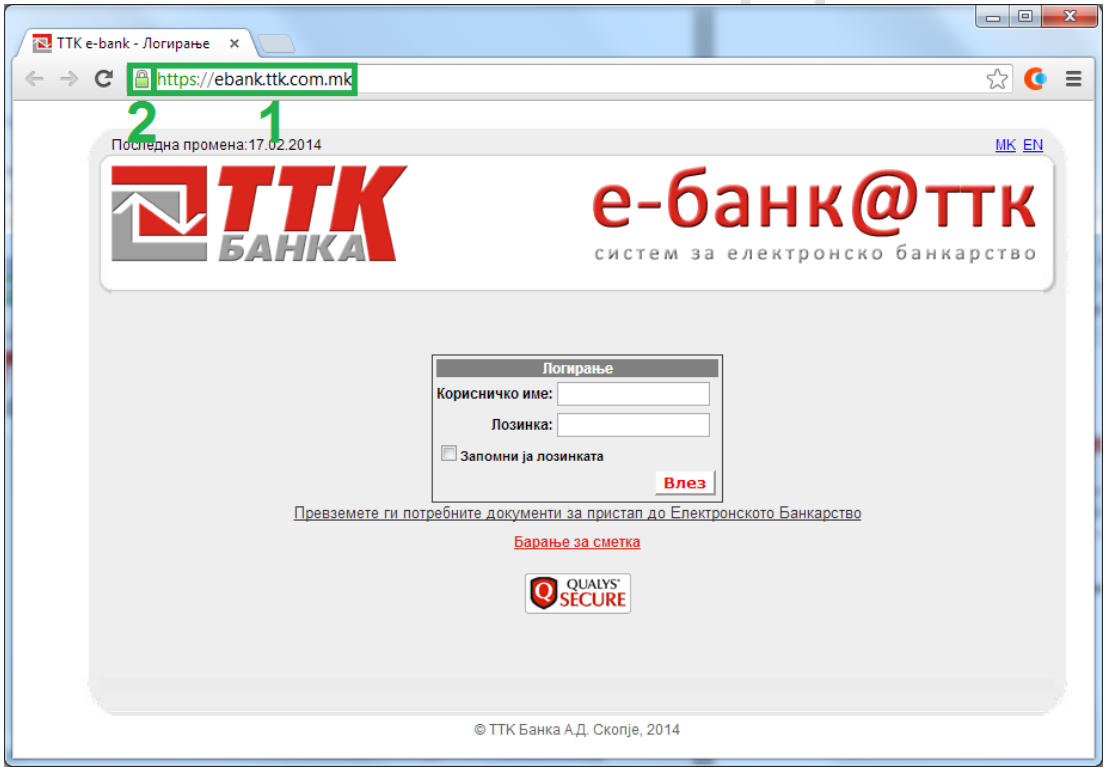
Слика 2 Извештај за безбедносните проверки на сајтот за електронско банкарство

ИДЕНТИФИКУВАЊЕ НА ЕЛЕКТРОНСКОТО БАНКАРСТВО

Комуникацијата помеѓу корисниците на електронското банкарство и Банката (https://ebank.ttk.com.mk) преку Интернет е со користење на безбедна 128 битна TLS 1.0 (Transport Layer Security) енкрипција (Слика 45 **(1)** и Слика 46 **(1)**) која гарантира високо ниво на сигурност.



Слика 3 Изглед на страната за најава на електронското банкарство на ТТК Банка АД Скопје во Internet Explorer

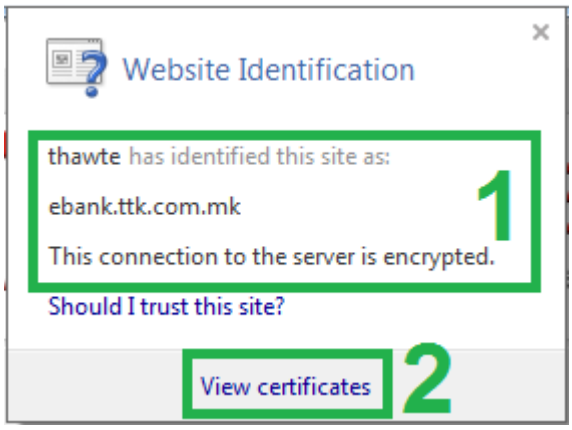


Слика 4 Изглед на страната за најава на електронското банкарство на ТТК Банка АД Скопје во Google Chrome

За потврдување на автентичноста, т.е. идентитетот на апликацијата на ТТК Банка наменета за електронско банкарство преку Интернет (https://ebank.ttk.com.mk), банката користи дигитален сертификат издаден од меѓународен изадавач на дигитални сертификати Thawte.

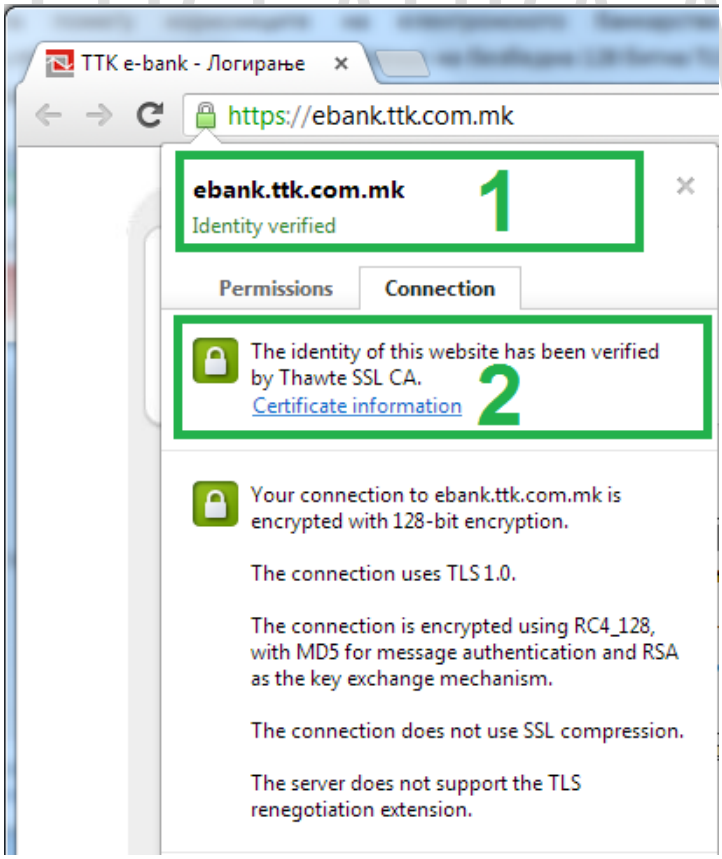
Корисникот на електронско банкарство може да изврши проверка на идентитетот (автентичноста) на електронското банкарство на ТТК Банка АД Скопје со кликнување на иконата за безбедност во адресната лента на пребарувачот (*Слика 3 Изглед на страната за најава на електронското банкарство на ТТК Банка АД Скопје во Internet Explorer*(2) и *Слика 4 Изглед на страната за најава на електронското банкарство на ТТК Банка АД Скопје во Google Chrome*(2)) .

Притоа се појавува следново известување кај Internet Explorer:



Слика 5 Информации за идентитетот на https://ebank.ttk.com.mk кај Internet Explorer

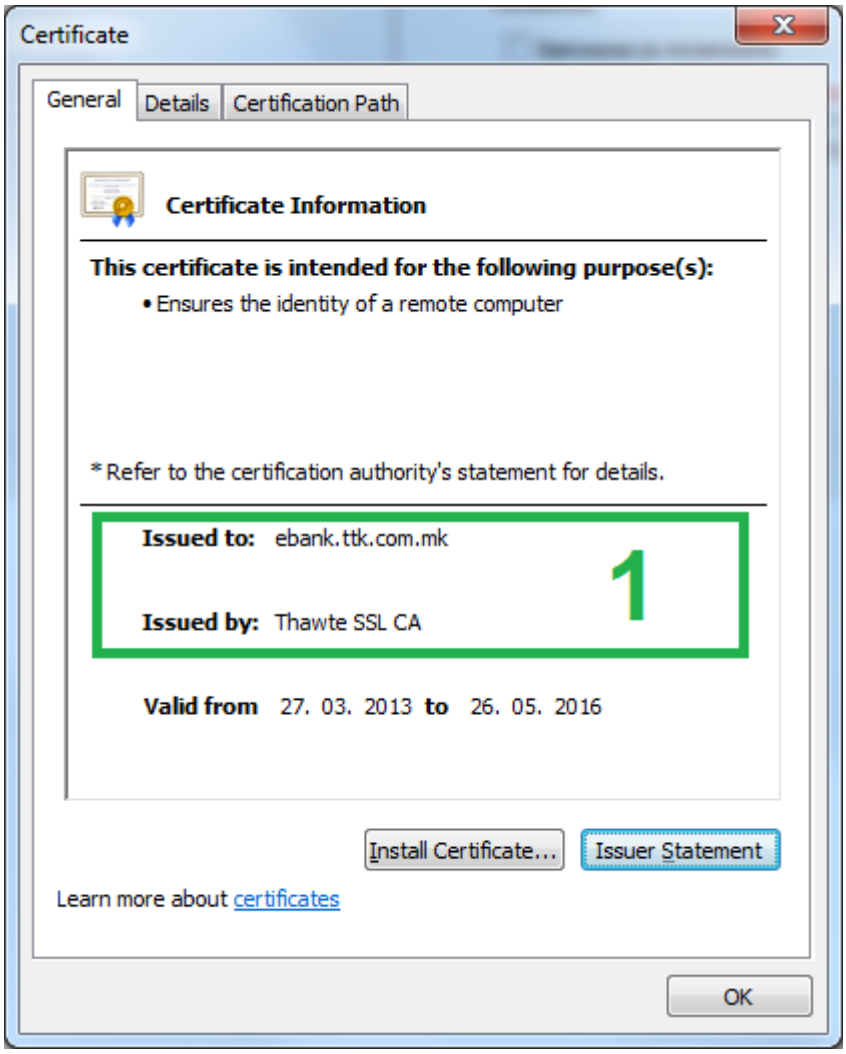
или кај Google Chrome:



Слика 6 Информации за идентитетот на https://ebank.ttk.com.mk кај Google Chrome

Од каде се гледа идентитетот на ebank.ttk.com.mk е потврден (верифициран) од страна на Thawte (*Слика 5 Информации за идентитетот на https://ebank.ttk.com.mk кај Internet Explorer* **(1)** и *Слика 6 Информации за идентитетот на https://ebank.ttk.com.mk кај Google Chrome* **(1)**).

Може да се прегледа и серверскиот сертификат за потврда на идентитетот на Банката - ebank.ttk.com.mk (*Слика 5 Информации за идентитетот на https://ebank.ttk.com.mk кај Internet Explorer* **(2)** и *Слика 6 Информации за идентитетот на https://ebank.ttk.com.mk кај Google Chrome* **(2)**) :



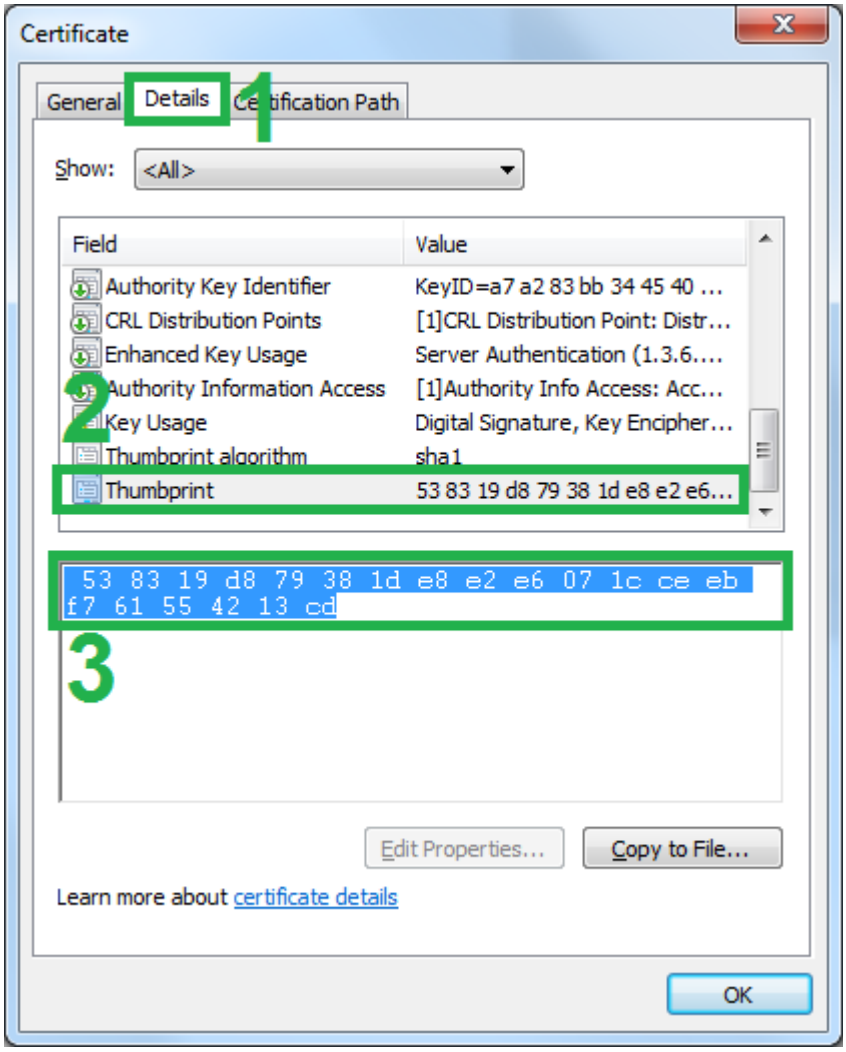
Слика 7 Податоци за серверскиот сертификат за идентификација на ebank.ttk.com.mk

Од каде може да се види дека серверскиот сертификат е издаден на ebank.ttk.com.mk од Thawte SSL CA (*Слика 7 Податоци за серверскиот сертификат за идентификација на ebank.ttk.com.mk* **(1)**).

Напомена: Thawte е меѓународно признаен авторитет за издавање на дигитални сертификати.

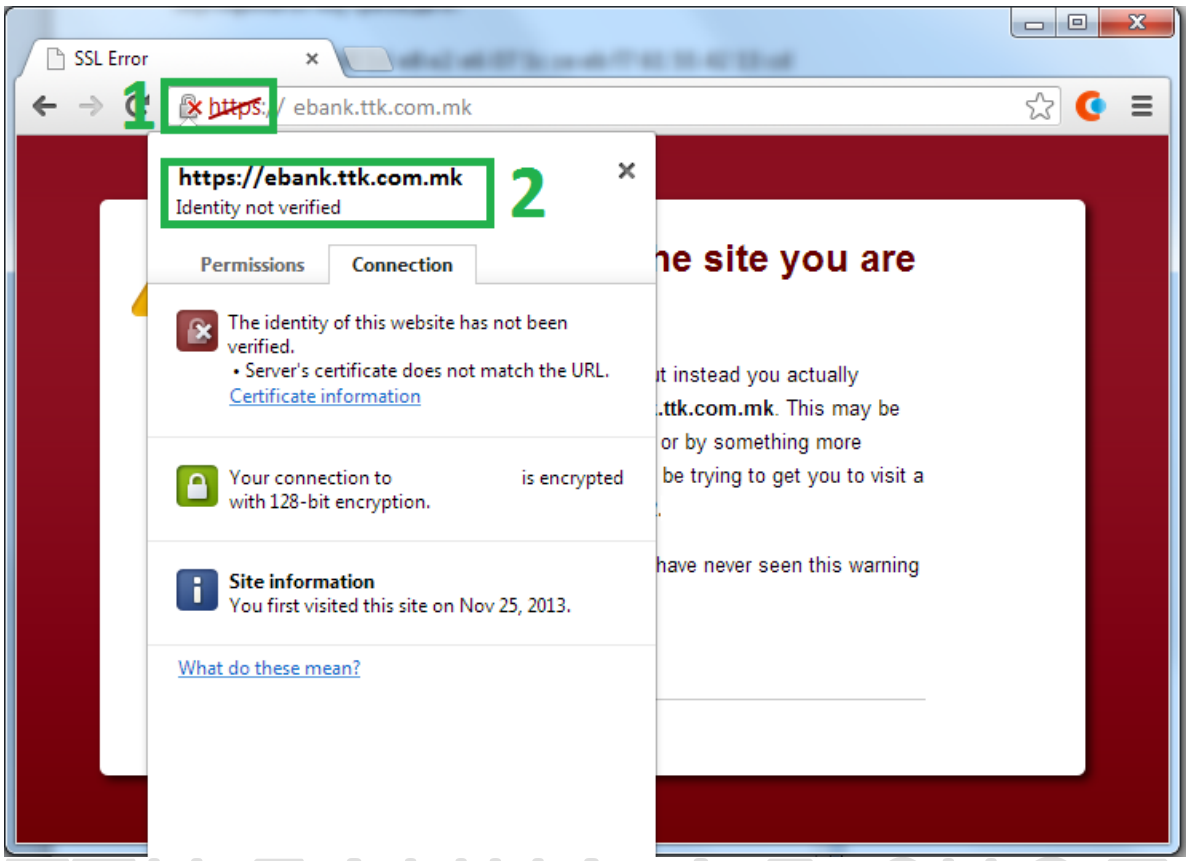
Дополнително, од деталите за серверскиот сертификат на ebank.ttk.com.mk (*Слика 8 Детали за серверскиот сертификат на ebank.ttk.com.mk*(1)) може да се види и провери неговата автентичност преку споредување на "Thumbprint" кодот (*Слика 8 Детали за серверскиот сертификат на ebank.ttk.com.mk* (2) (3)) на сертификатот кој треба да е:

53 83 19 d8 79 38 1d e8 e2 e6 07 1c ce eb f7 61 55 42 13 cd

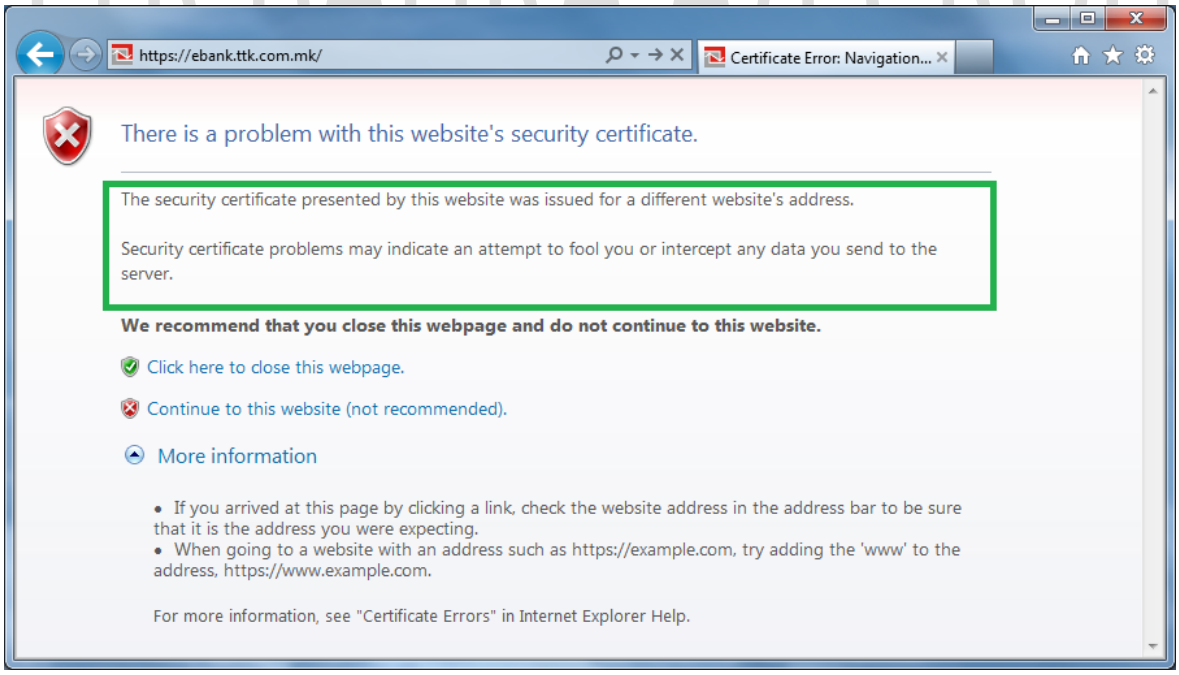


Слика 8 Детали за серверскиот сертификат на ebank.ttk.com.mk

Доколку при обид за најава на https://ebank.ttk.com.mk од страна на корисниците на електронското банкарство се појави известување како на наредните слики (*Слика 9 Проблем со препознавање на серверсиот сертификат на https://ebank.ttk.com.mk кај Internet Explorer* и *Слика 10 Проблем со препознавање на серверсиот сертификат на https://ebank.ttk.com.mk кај Google Chrome*) значи дека има проблем со успешното верифицирање на идентитетот на https://ebank.ttk.com.mk и од безбедносни причини се препорачува да се прекине со понатамаошната комуникација и да се извести ТТК Банка АД Скопје.



Слика 9 Проблем со препознавање на серверсиот сертификат на https://ebank.ttk.com.mk кај Internet Explorer



Слика 10 Проблем со препознавање на серверсиот сертификат на https://ebank.ttk.com.mk кај Google Chrome

КРАЖБА НА ИДЕНТИТЕТ

КРАЖБА И ЗЛОУПОТРЕБА ДА ИДЕНТИТЕТОТ НА КОРИСНИКОТ Е НЕДОЗВОЛЕНО КОРИСТЕЊЕ НА НЕКОИ ОД ПОДАТОЦИТЕ НА КОРИСНИКОТ СТЕКНАТИ НА РАЗЛИЧНИ НАЧИНИ, А СО НАМЕРА ЗА НЕОВЛАСТЕНО ЗДОБИВАЊЕ СО ИНФОРМАЦИИ ИЛИ ФИНАНСИСКИ СРЕДСТВА, ПРЕДИЗВИКУВАЊЕ НА МАТЕРИЈАЛНА ИЛИ РЕПУТАЦИСКА ШТЕТА И СЛИЧНО.

ПРИМЕРИ НА КРАЖБА И ЗЛОУПОТРЕБА НА ИДЕНТИТЕТ ВО ЕЛЕКТРОНСКОТО БАНКАРСТВО БИ БИЛЕ:

- ЗДОБИВАЊЕ И КОРИСТЕЊЕ НА ПОДАТОЦИТЕ ЗА ПРИСТАП И РАБОТА СО ЕЛЕКТРОНСКОТО БАНКАРСТВО (КОРИСНИЧКО ИМЕ И ЛОЗИНКА, ДИГИТАЛЕН СЕРТИФИКАТ И ЛОЗИНКА)
- НЕОВЛАСТЕНО ВРШЕЊЕ НА ТРАНСАКЦИИ ОД СМЕТКИТЕ НА КОРИСНИКОТ.
- ЗЛОУПОТРЕБА НА ИНФОРМАЦИИТЕ ЗА СМЕТКИТЕ И ПРОИЗВОДИТЕ НА КОРИСНИКОТ КАКО И НЕГОВИТЕ ЛИЧНИ ПОДАТОЦИ.

СОЦИЈАЛЕН ИНЖЕНЕРИНГ

СОЦИЈАЛНИОТ ИНЖЕНЕРИНГ КАКО ТАРГЕТ ГО ИМА КОРИСНИКОТ И ПРЕТСТАВУВА ОБИД ЗА НЕГОВА МАНИПУЛАЦИЈА КАКО БИ ОТКРИЛ ДОВЕРЛИВИ ПОДАТОЦИ КОИ НАПАЃАЧОТ ПОСЛЕ МОЖЕ ДА ГИ ИСКОРИСТИ ЗА СВОИ НЕЛЕГАЛНИ ЦЕЛИ. НАЈЧЕСТО ВО СОЦИЈАЛНИОТ ИНЖЕНЕРИНГ СЕ КОРИСТИ ЛАЖНО ПРЕТСТАВУВАЊЕ, НА ПРИМЕР ВО ИМЕ НА БАНКАТА, КАКО БИ СЕ ДОВЕЛ ВО ЗАБЛУДА КОРИСНИКОТ ДА ГО ИЗДАДЕ БАРАНИТЕ ПОДАТОЦИ.

MAN IN THE MIDDLE OF THE BROWSER

ПРЕКУ ОВАА ТЕХНИКА НА НАПАД, А КАКО РЕЗУЛТАТ НА ПРЕТХОДНА ЗАРАЗА НА НЕГОВИОТ КОМПЈУТЕР (BROWSER) СО ЗЛОНАМЕРЕН СОФТВЕР, КОРИСНИКОТ СЕ ДОВЕДУВА ВО ЗАБЛУДА ДЕКА КОМУНИЦИРА СО ОФИЦИЈАЛНИОТ САЈТ НА БАНКАТА, А ВСУШНОСТ КОМУНИРА СО СТРАНА НАМЕНЕТА ЗА КРАЖБА НА ДОВЕРЛИВИ ПОДАТОЦИ КАКО КОРИСНИЧКО ИМЕ, ЛОЗИНКА, БРОЈ НА КРЕДИТНА КАРТИЧКА И СЛИЧНО. ЗАТОА Е МНОГУ ВАЖНО КОРИСНИКОТ ДА ВРШИ ПРОВЕРКА НА ИДЕНТИТЕТОТ НА САЈТОТ ДО КОЈ ПРИСТАПУВА.

СИГУРНОСНИ НАПОМЕНИ ЗА КОРИСНИЧКОТО ИМЕ И ЛОЗИНКАТА

- КОМБИНАЦИЈАТА ОД КОРИСНИКО ИМЕ И ЛОЗИНКА Е САМО ЗА КОРИСНИКОТ И НЕ ТРЕБА ДА БИДЕ СПОДЕЛУВАНА СО ДРУГИ ЛИЦА.
- НЕ СЕ ПРЕПОРАЧУВА ЗАЧУВУВАЊЕ НА КОМБИНАЦИЈАТА ОД КОРИСНИЧКОТО ИМЕ И ЛОЗИНКАТА ВО ПРЕБАРУВАЧОТ ПРЕКУ КОЈ КОРИСНИКОТ ПРИСТАПУВА ДО ПОЧЕТНАТА СТРАНА ВО ЕЛЕКТРОНСКО БАНКАРСТВО.
- НЕ СЕ ПРЕПОРАЧУВА ЗАПИШУВАЊЕ НА КОМБИНАЦИЈАТА ОД КОРИСНИЧКО ИМЕ И ЛОЗИНКА.
- СЕ ПРЕПОРАЧУВА ПЕРИОДИЧНО (ИЛИ ПО ПОТРЕБА) МЕНУВАЊЕ НА ЛОЗИНКАТА.

- ПО ЗАВРШУВАЊЕТО СО АКТИВНОСТИТЕ, ЗАДОЛЖИТЕЛНО Е ПОТРЕБНО ДА СЕ ОДЈАВИТЕ ОД СИСТЕМОТ ЗА ЕЛЕКТРОНСКО БАНКАРСТВО.

СИГУРНОСНИ МЕРКИ ЗА КОРИСНИЧКИТЕ КОМПЈУТЕРИ

- КОРИСНИКОТ ЗА РАБОТА ПРЕКУ ЕЛЕКТРОНСКО БАНКРСТВО ТРЕБА ДА КОРИСТИ БЕЗБЕДНИ КОМПЈУТЕРИ КОИ СЕ ОДРЖУВААТ ОД АДМИНИСТРАТОРИ ВО КОИ КОРИСНИКОТ ИМА ДОВЕРБА.
- НЕ КОРИСТИТЕ ЈАВНИ КОМПЈУТЕРИ ЗА ПРИСТАП ДО ЕЛЕКТРОНСКОТО БАНКАРСТВО ИЛИ КОМПЈУТЕРИ ДО КОИ ПРИСТАП ИМААТ РАЗНИ ЛИЦА.
- СЕ ПРЕПОРАЧУВА КОРИСТЕЊЕ НА ЛЕГАЛНИ ВЕРЗИИ НА ОПЕРАТИВНИ СИСТЕМИ И АПЛИКАТИВЕН СОФТВЕР КОИ РЕДОВНО СЕ НАДГРАДУВААТ СО НАЈНОВИТЕ ВЕРЗИИ ИЗДАДЕДИ ОД ПРОИЗВОДИТЕТИЛЕТЕ НА СОФТВЕР.
- СЕ ПРЕПОРАЧУВА КОРИСТЕЊЕ НА АНТИВИРУСНИ ПАКЕТИ И ПОСТОЈАНА НАДГРАДБА НА НИВНИТЕ БАЗИ.

СИГУРНОСТ НА ДИГИТАЛНИОТ СЕРТИФИКАТ

- ИНСТАЛИРАЈТЕ ГО ДИГИТАЛНИОТ СЕРТИФИКАТ САМО НА КОМПЈУТЕРИТЕ ДО КОИ ИМАТЕ ПРИСТАП САМО ВИЕ И ЕВЕНТУАЛНО ДРУГИ ЛИЦА ВО КОИ ИМАТЕ ДОВЕРБА.
- ПРИ ИНСТАЛАЦИЈАТА НА ДИГИТАЛНИОТ СЕРТИФИКАТ ЗАДОЛЖИТЕЛНО КОРИСТЕТЕ ВИСОКО НИВО НА СИГУРНОСТ НА СЕРТИФИКАТОТ (ENABLE STRONG PRIVATE KEY PROTECTION) ОДНОСНО ПРИ СЕКОЕ КОРИСТЕЊЕ НА СЕРТИФИКАТОТ ДА БАРА ЛОЗИНКА.
- ЛОЗИНКАТА НА ДИГИТАЛНИОТ СЕРТИФИКАТ ИСТО КАКО И ЛОЗИНКАТА ЗА НАЈАВА НА ЕЛЕКТРОНСКОТО БАНКАРСТВО НЕ ТРЕБА ДА ЈА СПОРЕДЕЛУВАТЕ СО ДРУГИ ЛИЦА ИЛИ ДА ЈА ЗАПИШУВАТЕ НА МЕСТА ДО КОИ МОЖЕ ДА ДОБИЈАТ ПРИСТАП НЕОВЛАСТЕНИ ЛИЦА.
- НЕ ГО ИНСТАЛИРАЈТЕ ДИГИТАЛНИОТ СЕРТИФИКАТ НА ЈАВНИ КОМПЈУТЕРИ.
- НЕ ГО ПРЕПРАЌАЈТЕ Е-МАИЛ-ОТ СО ДИГИТАЛНИОТ СЕРТИФИКАТ НА НИКОЈ.
- ВО СЛУЧАЈ НА СОМНЕНИЕ ДЕКА Е КОМПРОМИТИРАН ВАШИОТ ДИГИТАЛЕН СЕРТИФИКАТ ВЕДНАШ ПОБАРАЈТЕ ОД БАНКАТА НЕГОВО БЛОКИРАЊЕ.

ОСТАНАТИ СИГУРНОСНИ НАПОМЕНИ

- БАНКАТА НА НИТУ ЕДЕН НАЧИН (ПРЕКУ ТЕЛЕФОН, E-MAIL ИЛИ ФОРМА РАЗЛИЧНА ОД ФОРМАТА ЗА НАЈАВА НА ЕЛЕКТРОНСКО БАНКАРСТВО) НЕМА ДА ПОБАРА ЧУСТВИТЕЛНИТЕ ИНФОРМАЦИИ КАКО ШТО СЕ КОРИСНИЧКОТО ИМЕ И ЛОЗИНКАТА ЗА НАЈАВА НА ЕЛЕКТРОНСКО БАНКАРСТВО, ДИГИТАЛНИОТ СЕРТИФИКАТ ИЛИ ЛОЗИНКАТА ЗА ДИГИТАЛНИОТ СЕРТИФИКАТ. ДОКОЛКУ НЕКОЈ ВИ ГИ БАРА ОВИЕ ПОДАТОЦИ НА БИЛО КОЈ НАЧИН ТОГАШ ВЕРОЈАТНО ПРЕТСТАВУВА ОБИД ЗА КРАЖБА НА ПОДАТОЦИ И ВАКВИОТ СЛУЧАЈ ТРЕБА ДА БИДЕ ПРИЈАВЕН ВО БАНКАТА.
- НИКОГАШ НЕ КОРИСТИТЕ ЛИНКОВИ ОД ТРЕТИ СТРАНИ КОИ ТВРДАТ ДЕКА ВОДАТ ДО СТРАНАТА ЗА НАЈАВА НА ЕЛЕКТРОНСКОТО БАНКАРСТВО https://ebank.ttk.com.mk .

- ПО НАЈАВАТА НА ЕЛЕКТРОНСКО БАНКАРСТВО СТОИ ПОДАТОК ЗА ПОСЛЕДЕН ПАТ КОГА СТЕ ГО КОРИСТЕЛЕ СИСТЕМОТ. ДОКОЛКУ ОВОЈ ПОДАТОК НЕ СООДЕЈСТВУВА НА ДАТУМОТ И ВРЕМЕТО КОГА СЕ ИМАТЕ НАЈАВЕНО ПОСЛЕДЕН ПАТ ЗАДОЛЖИТЕЛНО ИЗВЕСТЕТЕ ЈА БАНКАТА И ИЗВРШИТЕ ПРОМЕНА НА ЛОЗИНКАТА.
- ВРШЕТЕ РЕДОВНА ПРОВЕРКА НА СОСТОЈБАТА И ТРАНСКАЦИИТЕ НА ВАШИТЕ СМЕТКИ ВО БАНКАТА И ДОКОЛКУ ЗАБЕЛЕЖИТЕ ОПРЕДЕЛЕНИ НЕЛОГИЧНОСТИ ВЕДНАШ ИЗВЕСТЕТЕ ЈА БАНКАТА.