




**Polski Związek Krótkofalowców
Administrator systemów informatycznych PZK**

Certyfikat AlphaSSL DV SSL wildcard dla domeny pzk.org.pl. (08.2018)

Od dnia 03.08.2015 r. wszystkie serwery PZK – serwer obsługujący główną domenę pzk.org.pl oraz serwery używające subdomen domeny pzk.org.pl (wszystkie domeny oddziałów terenowych PZK, domeny serwerów tematycznych, itp.) były objęte certyfikatem SSL. PZK zakupiło komercyjny certyfikat SSL dla serwera / serwerów PZK.

Zakupiony certyfikat Commercial SSL jest tzw. certyfikatem "wildcard" i został zakupiony z okresem ważności na 3 lata. Certyfikat Commercial SSL jest (był) kompromisem ceny i jakości i jest (był) w zupełności wystarczający na potrzeby Polskiego Związku Krótkofalowców.

Od dnia 2.08.2018 r. dotychczasowy certyfikat Commercial SSL firmy Unizeto / Certum został zastąpiony jako kontynuacja certyfikatem ALPHASSL firmy GlobalSign.  <https://www.globalsign.com/en/>). Powodem rezygnacji z certyfikatu Unizeto była niekonkurencyjność cenowa. Od 2018 wszystkie światowe certyfikaty SSL wydawane są tylko i wyłącznie na 1 rok lub na 2 lata.

Zakupione certyfikaty jw. są tzw. certyfikatami typu DV (domain validated). Autentykacja takich certyfikatów odbywa się poprzez autoryzację dostępu do posiadanej domeny (w naszym przypadku domeny „pzk.org.pl”). Certyfikaty typu DV są najtańszymi certyfikatami i jednocześnie proces ich wydawania jest najszybszy.

Certyfikat SSL i co to oznacza w praktyce? Odpowiedź jest bardzo prosta - wszystkie dane przekazywane z serwerów i do serwerów objętych certyfikatem SSL z urządzeń końcowych użytkownika objęte są szyfrowaniem i nie jest możliwy ich nieuprawniony podgląd. Z głównym portalem PZK jest zintegrowany Elektroniczny System Ewidencji Członków PZK (tzw. O.S.E.C.). System ten jest obsługiwany przez wszystkie OT PZK (przez uprawnione osoby z zarządów OT PZK – skarbnik, sekretarz).

Ponadto posiadanie certyfikatu SSL wildcard umożliwia objęcie połączeniami szyfrowanymi portali wszystkich OT PZK mających swoje portale na serwerach PZK. OT PZK mogą (i powinny) używać połączeń szyfrowanych. Implementacja tego jest oczywiście zadaniem dla administratorów serwerów OT PZK, które to znajdują się w zasobach informatycznych PZK. Wsparcia administratorom OT PZK udziela Administrator SI PZK.

Jeżeli ktoś jest zainteresowany bliżej sprawami właściwości certyfikatów, jakości serwerów w połączeniu z certyfikatami SSL oraz implementacją protokołów transmisji może skorzystać z wielu bezpłatnych narzędzi znajdujących się w sieci Internet.

Sprawdzenie jakości certyfikatu (a także ceny certyfikatów):
<https://certyfikatyssl.pl/ssl-tools/check-ssl-certificate.html>

https://certyfikatyssl.pl/certificates_comparison.html

Sprawdzenie jakości certyfikatu oraz kompleksowa analiza protokołów transmisji serwera, przeglądarki i innych parametrów:

<https://www.ssllabs.com/> - QUALYS SSL Labs

<https://www.ssllabs.com/ssltest/> - sprawdzenie serwera

<https://www.ssllabs.com/ssltest/viewMyClient.html> - sprawdzenie przeglądarki

Zygmunt Szumski SP5ELA
Administrator portalu PZK
admin@pzk.org.pl
Warszawa, dnia 05.08.2018 r.