

Instrukcja wdrożenia usług bezpieczeństwa OSE

Przeznaczona dla komputerów z systemem Windows w wersji 7,8,10



ose.gov.pl

Spis treści

Spis treści	2
O projekcie Ogólnopolskiej Sieci Edukacyjnej	3
Wstęp	3
Instrukcja instalacji certyfikatów SSL na komputerach z systemem Windows	4
1. Automatyczna instalacja certyfikatów SSL dla wszystkich przeglądarek na komputerach z Windows.	5
2. Manualna instalacja certyfikatów SSL na komputerach z Windows dla przeglądarek Chrome, EDGE, Internet Explorer, Opera	9
3. Manualna instalacja certyfikatów SSL na komputerach z Windows dla przeglądarki Mozilla Firefox	13

O projekcie Ogólnopolskiej Sieci Edukacyjnej

Ogólnopolska Sieć Edukacyjna (zwana dalej "OSE") jest projektem konstytuowanym na mocy ustawy z dnia 27 października 2017r. o Ogólnopolskiej Sieci Edukacyjnej (zwanej dalej "Ustawą").

Zgodnie z Ustawą, OSE jest publiczną siecią telekomunikacyjną, dzięki której szkoły otrzymają nieodpłatny dostęp do szybkiego internetu wraz z usługami bezpieczeństwa sieciowego i teleinformatycznego oraz usługami ułatwiającymi dostęp do technologii cyfrowych.

Operatorem OSE jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (zwany dalej "NASK"), nadzorowany przez Ministra Cyfryzacji.

Wstęp

6

W niniejszej instrukcji opisane zostały czynności wymagane do prawidłowego uruchomienia zamówionych przez szkołę zaawansowanych usług bezpieczeństwa OSE:

- Ochrona przed szkodliwym oprogramowaniem
- Ochrona Użytkownika OSE

Usługi bezpieczeństwa OSE realizowane są na urządzeniach centralnych w sieci OSE. Do ich poprawnego działania wymagana jest inspekcja ruchu szyfrowanego SSL. W tym celu niezbędne jest zainstalowanie certyfikatów SSL, które udostępnia NASK. Zainstaluj je na wszystkich komputerach i urządzeniach przenośnych (laptopy, tablety, smartfony) łączących się z siecią OSE.

W przypadku podłączenia do sieci szkolnej urządzenia nie mającego zainstalowanego certyfikatu SSL (zarówno komputera jak i innych urządzeń przenośnych), usługi bezpieczeństwa nie będą działały prawidłowo, utrudnione będzie korzystanie z internetu na tym urządzeniu, większość stron www będzie wyświetlana nieprawidłowo, lub w ogóle może nie być wyświetlana.

Poprawne wykonanie czynności w niniejszej instrukcji zagwarantuje możliwość prawidłowego korzystania z zasobów internetu w sposób bezpieczny dla użytkowników sieci w szkole. Szczegółowe informacje dotyczące usług bezpieczeństwa w sieci OSE, znajdują się na portalu OSE, pod adresem <u>ose.gov.pl/uslugi-dodatkowe</u>.

Instrukcja instalacji certyfikatów SSL na komputerach z systemem Windows

6

Niniejsza Instrukcja opisuje trzy możliwe sposoby instalacji certyfikatów na komputerach z systemem Windows w szkole:

- 1. Automatyczny wykonywany na komputerach z systemem Windows 7,8,10 za pomocą dostarczonej przez NASK aplikacji instalatora. To jest zalecana metoda, w przypadku jej niepowodzenia, należy wykonać instalacje opisane w punktach 2, 3.
- 2. Manualny wykonywany na komputerach z Windows 7,8,10 dla przeglądarek Chrome, EDGE, Internet Explorer, Opera.
- Manualny wykonywany na komputerach z Windows 7,8,10 dla przeglądarki Mozilla Firefox.

Aplikacja, certyfikat wraz z niniejszą instrukcją dostępne są na stronie <u>certyfikat.ose.gov.pl</u>. W celu pobrania plików, otwórz przeglądarkę stron www na urządzeniu, na którym zamierzasz zainstalować certyfikat, otwórz powyższą stronę, wyszukaj sekcję poświęconą komputerom z systemem Windows a następnie kliknij na Pobierz pliki.

1. Automatyczna instalacja certyfikatów SSL dla wszystkich przeglądarek na komputerach z Windows.

Dostarczona przez NASK aplikacja instaluje certyfikaty SSL w sposób automatyczny dla wszystkich przeglądarek www (testowane na przeglądarkach: Microsoft Edge, Mozilla Firefox, Chrome, Opera) oraz dla wszystkich aktywnych w systemie kont użytkowników. Konta użytkowników założone w przyszłości również zostaną objęte ochroną w sposób całkowicie automatyczny.

Aby automatycznie zainstalować certyfikaty SSL za pomocą instalatora wykonaj następujące czynności:

- 1. Zapisz plik *pliki_windows.zip* na pulpicie komputera (lub użyj do tego celu pendrive'a), na którym certyfikat ma być zainstalowany.
- 2. Rozpakuj plik *pliki_windows.zip*.

6

3. Otwórz nowopowstały katalog cert.



4. Uruchom plik *cert_install.msi* z uprawnieniami administracyjnymi komputera lokalnego. Następnie potwierdź jego uruchomienie.

^{Kontrola konta użytkownika} Czy chcesz zezwolić tej od nieznanego wydawo zmian na tym urządzen	× aplikacji pochodzącej zy na wprowadzenie iu?
D:\cert\cert_install.msi Wydawca: Nieznany Pochodzenie pliku: Nośnik wyn Pokaż więcej szczegółów	Nienny w tym komputerze
Tak	Nie

5. Poczekaj aż program zainstaluje się.

6



6. Po poprawnie zakończonej instalacji w obszarze powiadomień pojawi się ikona zielonej tarczy, która oznacza, że certyfikat OSE został poprawnie zainstalowany, komputer jest chroniony przez usługi bezpieczeństwa OSE.



7. Po dwukrotnym kliknięciu ikony tarczy zaakceptuj poniższy komunikat, (dotyczy konta z uprawnieniami administracyjnymi).

Kontrola konta użytkownika Czy chcesz zezwolić tej od nieznanego wydawo zmian na tym urządzen	× aplikacji pochodzącej zy na wprowadzenie iu?
OSECertChecker.exe Wydawca: Nieznany Pochodzenie pliku: Dysk twardy Pokaż więcej szczegółów	y w tym komputerze
Tak	Nie

Otworzy się wtedy okno programu ze statusem działania usług bezpieczeństwa OSE oraz dostępnymi opcjami: *Odinstaluj* i *Ustawienia zaawansowane*



6

8. Gdy certyfikaty bezpieczeństwa OSE są poprawnie zainstalowane na danym urządzeniu, wyświetla się status: Twój internet OSE jest bezpieczny. Opcja *Odinstaluj* spowoduje usunięcie certyfikatu OSE z systemu Windows. W oknie zostanie wtedy wyświetlony komunikat *Twój internet OSE jeszcze nie jest bezpieczny*, ikona tarczy w obszarze powiadomień zmieni kolor na *czerwony*.





9. W Ustawieniach zaawansowanych możesz odznaczyć opcję Uruchamiaj aplikację Bezpieczny Internet OSE wraz ze startem Windows. Spowoduje to, iż program nie będzie włączał się przy każdym starcie systemu Windows, a konta użytkowników założone w przyszłości nie zostaną objęte ochroną w sposób automatyczny.

6



2. Manualna instalacja certyfikatów SSL na komputerach z Windows dla przeglądarek Chrome, EDGE, Internet Explorer, Opera.

Jeśli korzystasz z przeglądarek Chrome, EDGE, Internet Explorer, Opera i chcesz ręcznie zainstalować certyfikat SSL dostarczony przez NASK, wykonaj następujące czynności:

- 1. Zapisz plik *pliki_windows.zip* na pulpicie komputera, na którym certyfikat ma być zainstalowany (lub użyj do tego celu pendrive'a).
- 2. Rozpakuj plik *pliki_windows.zip*.

6

- 3. Otwórz nowopowstały katalog cert.
- 4. Kliknij dwukrotnie na plik certyfikatu (*certyfikat.crt*).
- 5. W oknie Certyfikat kliknij przycisk Zainstaluj certyfikat.

💀 Certyfikat	×
Ogólne Szczegóły Ścieżka certyfikacji	
Informacje o certyfikacie	-
Ten główny certyfikat urzędu certyfikacji nie jest zaufany. Aby ustanowić zaufanie, zainstaluj ten certyfikat w magazynie zaufanych głównych urzędów certyfikacji.	
Wystawiony dla: NASK PIB ROOT CA	
Wystawiony przez: NASK PIB ROOT CA	
Ważny od 22.05.2018 do 17.05.2038	
Zainstaluj certyfikat Oświadczenie wystawcy	
OK	

 W oknie *Kreator importu certyfikatów,* w sekcji *Lokalizacja przechowywania* wybierz opcję *Komputer lokalny* i kliknij przycisk Dalej (Next). Uwaga: Do wykonania polecenia konieczne będzie podanie poświadczeń użytkownika z

uprawnieniami administracyjnymi komputera lokalnego.

Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów. Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości uzytkownika i zawiera informacje używane do odrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, którym przechowywane są certyfikaty. Lokalizacja przechowywania Bieżący użytkownik Bieżący użytkownik Komputer lokalny	Kreator importu certy	rfikatów — Zapraszamy!
Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, którym przechowywane są certyfikaty. Iokalizacja przechowywania O Bieżący użytkownik	Ten kreator pozwala kopiować cer odwołania certyfikatów z dysku tv	tyfikaty, listy zaufania certyfikatów oraz listy wardego do magazynu certyfikatów.
Komputer lokalny	Certyfikat, wystawiany przez urzz użytkownika i zawiera informacje i bezpiecznych połączeń sieciowych w którym przechowywane są cert Lokalizacja przechowywania O Bieżący użytkownik	4d certyfikacji, stanowi potwierdzenie tożsamości używane do ochrony danych lub do ustanawiania 1. Magazyn certyfikatów jest obszarem systemowym, yfikaty.
Aby kontynywysé, kiknii przyciek Dalaj	Komputer lokalny	Dalet

6

7. W oknie Magazyn certyfikatów kliknij opcję Umieść wszystkie certyfikaty w następującym magazynie i w oknie, które pojawi się po kliknięciu przycisku Przeglądaj wybierz opcję Zaufane główne urzędy certyfikacji, kliknij OK a następnie kliknij przycisk Dalej (Next).

Magazyn certyfikatów		
Magazyny certyfikatów	to obszary systemowe, w któr	ych przechowywane są
System Windows może a określić inną lokalizację c O Automatycznie wy O Umieść wszystkie Wybieranie magazynu certyfik	uutomatycznie wybrać magazy Ila certyfikatu. /bierz magazyn certyfikatów n certyfikaty w następującym m atów X	n certyfikatów; możesz jednak a podstawie typu certyfikatu agazynie Przeglądaj
Wybierz magazyn certyfikatów, k	ctórego chcesz użyć.	
Wybierz magazyn certyfikatów, k Osobisty Zaufane główne urzędy Zaufanie przedsjebiorst	tórego chcesz użyć.	
Wybierz magazyn certyfikatów, k Osobisty Zaufane główne urzędy Zaufanie przedsiębiorst Pośrednie urzędy certyl Zaufani wydawcy Zaufani wydawcy	ttórego chcesz użyć.	

8. W oknie *Kończenie pracy Kreatora importu certyfikatów* sprawdź, czy podane informacje są dokładne, a następnie kliknij przycisk *Zakończ.*

6

	czenie pracy Kreatora	importu certy	fikatów	
Certyf	kat zostanie zaimportowany po kli	knięciu przycisku Zako	ńcz.	
Wybra	ne zostały następujące ustawienia	3:		
Maga Zawa	zyn certyfikatów wybrany przez u rtość	żytkownika Zaufane Certyfik	główne urzędy cer at	rtyfika
<				

9. Pomyślny import certyfikatu zostanie potwierdzony komunikatem kończącym pracę kreatora.



Aby dodatkowo sprawdzić czy certyfikat SSL został poprawnie zainstalowany do systemowego magazynu certyfikatów systemu Windows, należy wykonać poniższe kroki:

1. Otwórz przeglądarkę Internet Explorer

6

- Z paska *menu* wybierz *Narzędzia* -> *Opcje internetowe.* Jeśli pasek menu jest niewidoczny naciśnij na chwilę klawisz lewy *Alt+X.* Alternatywnie można kliknąć przycisk narzędzia zlokalizowany w prawym górnym rogu okna programu i także wybrać *Opcje internetowe.*
- 3. W oknie Opcje internetowe wybierz zakładkę Zawartość i kliknij przycisk Certyfikaty.

Połącz	enia	Progra	my	Zaa	wansowane
Ogólne	Zab	ezpieczenia	Pryv	vatność	Zawarto
Certyfikaty	Używanie o identyfikac	certyfikatów do ji.	połączeń	szyfrowany	ch i
Wyca	ryść stan <u>S</u>	SL <u>C</u> er	tyfikaty	V	/y <u>d</u> awcy
Autouzupeł	nianie –				
	Funkcja Au przechowu stron sieci dopasowar	itouzupełnianie ije poprzednie v Web i sugeruje nia.	vpisy ze	U	tawienia
Canały info	rmacyjne i	obiekty Web Sli	ce		
5	Kanały info aktualizow być odczyt programac	ormacyjne i obie aną zawartość : ana w program h.	kty Web S z witryn in ie Interne	Slice zapewn iternetowych t Explorer i v	ają 1, która może / innych
				Lie	tawionia
				0.	L <u>a</u> wieriia

4. W oknie *Certyfikaty* wybierz zakładkę *Zaufane główne urzędy certyfikacji*, powinien być widoczny wpis *NASK PIB ROOT CA*.

	11154	.,					
nne osoby Pośre	ednie urzę	dy certyfikacji	Zaufane g	łówne urzędy (certyfikacji	Zaufani v	4
Wystawiony dla		Wystawiony pr	zez	Data wyg	Przyjazna	nazwa	1
Microsoft Roo	ot Aut	Microsoft Root	Authority	31.12.2020	Microsoft	Root A	
Microsoft Roo	ot Cert	Microsoft Root	Certifi	10.05.2021	Microsoft	Root C	
Microsoft Roo	ot Cert	Microsoft Root	Certifi	24.06.2035	Microsoft	Root C	
Microsoft Roo	ot Cert	Microsoft Root	Certifi	23.03.2036	Microsoft	Root C	
NASK PIB RO	IOT CA	NASK PIB ROO	T CA	17.05.2038	<brak></brak>		
	ACC	NO LIABILITY	ACCEP	08.01.2004	VeriSign Ti	ime St	
QuoVadis Ro	ot CA 2	QuoVadis Root	CA 2	24.11.2031	QuoVadis	Root C	
QuoVadis Ro	ot CA	QuoVadis Root	CA 2 G3	12.01.2042	QuoVadis	Root C	
QuoVadis Ro	ot Cer	QuoVadis Root	Certifi	17.03.2021	QuoVadis	Root C	1
Importuj	ksportuj	. <u>U</u> suń			Za	aawansowa	ane
lamierzone cele ce	ertyfikatu						
<wszyscy></wszyscy>					[<u>W</u> yświet	ł

3. Manualna instalacja certyfikatów SSL na komputerach z Windows dla przeglądarki Mozilla Firefox.

Jeśli korzystasz z przeglądarki Mozilla Firefox i chcesz ręcznie zainstalować certyfikat SSL dostarczony przez NASK, wykonaj następujące czynności:

- 1. Zapisz plik *pliki_windows.zip* na pulpicie komputera, na którym certyfikat ma być zainstalowany (lub użyj do tego celu pendrive'a).
- 2. Rozpakuj plik pliki_windows.zip.

ტ

3. Z paska *Menu* wybierz *Narzędzia -> Opcje*. Jeśli pasek menu jest niewidoczny naciśnij na chwilę klawisz lewy *Alt.*

Alternatywnie można kliknąć przycisk menu \equiv zlokalizowany w prawym górnym rogu okna programu i wybrać **Opcje.**

\leftrightarrow	C U Firefox about:p	references	습	ŵ	•	
*	Ogólne	Ogólne				
Q	Wyszukiwanie	Uruchamianie				
≙ ₽	Prywatność i bezpieczeństwo Konto Firefoksa	 Sprawdzani<u>e</u>, czy Firefox je Firefox jest obecnie do 	st domyślną p omyślną przeg	rzegli Ilądai	ądark r <mark>ką</mark>	ą
		Po uruchomieniu programu Fire wyświetl stronę startową wyświetl pustą stronę wyświetl okna i karty z pop	fox: rzedniej <mark>s</mark> esji			

4. Z Menu po lewej stronie wybierz opcję *Prywatność i bezpieczeństwo* a następnie przewiń ekran do końca w dół.



5. Kliknij przycisk Wyświetl certyfikaty i wybierz zakładkę Organy certyfikacji.

	Menedžer certyfikatów						
Użytkownik	Osoby Serwery	Organy certyfika	cji Pozos	ałe			
Masz certyfika	ty, które identyfikują następu	ujące organy certyfika	icji:				
Nazwa certyfi	katu		Urządzeni	e zabezpieczające			
~4Sync Solutio	ons Sp. z o.oSKA						
osestatic.su	rfsafe.pl		Urządzenie	zabezpieczające			
oseproxy.su	urfsafe.pl		Urządzenie	zabezpieczające			
oseid.surfsa	ife.pl		Urządzenie	zabezpieczające			
✓AC Camerfirm	na S.A.						
Chambers	of Commerce Root - 2008		Builtin Obje	ect Token			
Global Cha	mbersign Root - 2008		Builtin Obje	ect Token			
		. Increased	Characteria	Harris Inde annumber 6 aufer 6			

6. Kliknij przycisk *Importuj* i wybierz dostarczony przez NASK certyfikat SSL.

-> -> -> -> Ten komputer	> Pulnit > Inst	nukcie i certyfikaty		a da Brarnikai	Instrukcie i certu	F 0		
Marco faldes	· · · uprc · · · · · ·	ungereergrinory		V O HILLIANS	Dre - m			
Duloit	^	News	^	Data and Ghavil	811 • L		Szukai w opciach	
- Folpic		TVd2Wd		Data modynkacji	typ		analog in opigation	
_88		certyfikat		22.05.2018 14:55	Certyhikat za	ibezpi		
×. 📙								×
2r								
a								
aa laatauluin i seet filostu	_							
Instructje i certynkaty	¥	<				>		
Nazwa pliku: cert	yfikat			 Pliki certyl 	ikatów	~		
				Otwór	z Anu	luj	ące	E \$
		VAC Camertirn	na S.A.			.11	1	^
	Bezp	Chambers of	of Commerce Root - 2008	Bui	Itin Object Tol	ken		
	Ochr	Global Char	mbersign Root - 2008	Bui	Itin Object Tol	ken		
		~AC Camerfirm	na SA CIF A82743287					
	· <u>0</u>	Camerfirma	Chambers of Commerce Root	Bui	Itin Object Tol	ken		
	*	Camerfirma	Global Chambersign Root	Bui	Itin Object Tol	ken		
	~	~ACCV						
		ACCVRAI71		Bui	Itin Object Tol	ken		
	Certy	vActalis S n A	03358520967					
	Kiedy	·····		[]				
	w	Wyswietl	Edytuj ustawienia zaufania	Importuj <u>Eksp</u>	ortuj <u>U</u> s	un lub pi	rzestan ufać	
								OK
	🔍 D							

 W następnym oknie potwierdź zaufanie dla certyfikatu SSL (należy zaznaczyć oba checkboxy, tzn. Zaufaj temu CA przy identyfikacji witryn internetowych, oraz Zaufaj temu CA przy identyfikacji użytkowników poczty)

i kliknij **OK.**

6

		Mene	dżer certyfikat	ów		
[Pobieranie certyfikatu			×		
Użytkov	Otrzymano prośbę o dołączenie nowego or	anów.				
Masz certy	Czy zakwalifikować "NASK - Państwowy Instytut Badawczy" jako źródło godne zaufania w następujących przypadkach?					
Nazwa ce	Zaufaj temu CA przy identyfikacji witryn internetowych.			ce		
~4Sync So	Zaufaj temu CA przy identyfikacji użytko	wników poczty.				
osestat osepro:	Jeżeli jest to możliwe, przed udzieleniem zgody należy zapoznać się z certyfikatem tego organu oraz jego polityką i stosowanymi procedurami.					
oseid.su	Wyświetl Sprawdź certyfikat CA			2		
✓AC Came Chamb.			OK	Anuluj		
Global (Chambersign Root - 2008		Builtin Obje	ect Token		
			There extend	Hand July summaries for the f		

6

8. Po pomyślnym dodaniu certyfikatu SSL, pojawi się on na liście dostępnych i zaufanych organów certyfikacji.

Menedźer certyfikatów					
Użytkownik Osoby Serwery	Organy certyfikacji	Pozostałe			
Masz certyfikaty, które identyfikują następują	ce organy certyfikacji:				
Nazwa certyfikatu		Urządzenie zabezpieczające			
~MSIT Machine Auth CA 2					
MSIT Machine Auth CA 2	Urządzenie zabezpieczające				
NASK - Państwowy Instytut Badawczy					
NASK - Państwowy Instytut Badawczy	U	Irządzenie zabezpieczające			
~NetLock Kft.					
NetLock Arany (Class Gold) Főtanúsítvány	В	Builtin Object Token			
NetLock OnlineSSL (Class Online) Tanúsítva	ánykiadó U	Irządzenie zabezpieczające			
Wućwioti Edutuj ustawionja zaufanja	Importui	portui			

- 9. Kliknięcie **OK** kończy proces dodawania certyfikatu SSL, można zamknąć zakładkę **Opcje**.
- 10. Powyższą instrukcję należy powtórzyć dla każdego użytkownika systemu Windows korzystającego z przeglądarki Mozilla.

(Powyżej umieszczone zrzuty ekranów zostały wykonane na wersji programu 62.0 (64 bity)

T +48 22 182 55 55 ose@ nask.pl

A ul. Kolska 12 - 01-045 Warszawa

W ose.gov.pl

NIP 5210417157 REGON 010464542





Rzeczpospolita Polska



Unia Europejska Europejski Fundusz Rozwoju Regionalnego





Ministerstwo Cyfryzacji

