Робота із сертифікатом від Globalsign

Отримання сертифікату Підписування документів MS Word Надсилання підписаних та шифрованих повідомлень з допомогою The Bat

Зміст

Отримання сертифікату від Globalsign	3
Експорт сертифікату у файл	19
Імпорт сертифіката від GlobalSign	30
Здійснення імпорту сертифікату від GlobalSign в Internen Exploler	30
Здійснення імпорту сертифікату від GlobalSign в TheBat	36
Використання сертифікату від GlobalSign для накладання електронного цифрового підпису в документах MS Word	46
Підпис документів MS Word 2013	46
Підпис документів MS Word 2010	54
Підпис документів MS Word 97-2003	60
Використання сертифікату від GlobalSign для надсилання підписаних, зашифрованих, підисаних/зашифрованих листів з допомогою TheBat	70
Підписування листів сертифікатом від GlobalSign	70
Шифрування листів із використанням сертифікату від GlobalSign	75
Імпорт ключа в адресну книгу	76
Надсилання зашифрованого листа	82
Шифрування та накладання підпису із використанням сертифікату від GlobalSign	87
Надсилання підготованих до відправки листів	93

Отримання сертифікату від Globalsign

Для отримання сертифікату від Globalsign спершу слід зайти на сайт <u>https://www.globalsign.com/</u> (Див. Рис. 1, а.). При генерації сертифікату має значення яким саме браузером користуватися, тому процес генерації слід розпочати і закінчити на одному і тому ж комп'ютері із використанням одного і того ж браузера. Ми будемо використовувати **Google Chrome**¹. Процес генерації сертифікату для інших браузерів може дещо відрізнятися, тому їх можна використовувати більш досвідченим користувачам. Крім того рекомендується використовувати поштову скриньку на сервері **Gmail**.

Стартова сторінка Globalsign матиме приблизно такий вигляд (Див. Рис. 1):



Рис. 1 Приклад стартової сторінки Globalsign

Організація доволі часто міняє інтерфейс свого Web-сайту, тому з часом сторінка матиме інший вигляд.

Підведемо вказівник мишки до меню Products, для того, щоб перегляну перелік послуг (Див. Рис. 1, б). Серед запропонованого списку обираємо Digitally Sign and Encrypt Email (Див. Рис. 2), тобто обираємо можливість використання сертифікату для створення цифрового підпису та шифрування

¹ На момент опитування у групі заочників браузером Google Chrome користувалося найбільше студентів, тому він був вибраний в якості прикладу.

повідомлень електронної пошти. Проте, отриманий сертифікат також дасть можливість накладати електронний цифровий підпис і документам MS Office.

Products	SSL	Enterprise	Partners	About Us
GlobalSign	Products	Enterprise	Platforms	
SSL Certificates Code Signing PDF Signing		Enterprise F Managed S	РКІ SL	
Microsoft O Strong Aut	office Signing nentication	I need to:		
Email Secu Enterprise PersonalSig View all Glo	irity CA Root Signing gn Certificates obalSign Products	Manage Mu Digitally Sig Digitally Sig Digitally Sig Upload to F	Itiple SSL Certificates In Code and Applicati In and Encrypt Email In PDF and Microsoft DA Electronic Submi	s ions Office Docs ission Gateway

Рис. 2 Фрагмент. Меню "Products"

Після переходу за посиланням з'являється можливість згенерувати пробний сертифікат. Для цього слід натиснути кнопку "Free Trial" (Рис. 3).



Рис. 3 Кнопка "Free Trial"

Наступна сторінка, яка завантажиться матиме поле зі списком у якому слід вибрати регіон. Найчастіше пробний сертифікат можна отримати, якщо скористатися в якості регіону North America (United States & Canada) (Рис. 4, а). В інших регіонах сервіс використання пробних сертифікатів може не надаватися. Після вибору регіону слід натиснути кнопку "Select and Continue" (Рис. 4, б).



Рис. 4 Вибір регіону

Буде розпочато процес обробки замовлення (Рис. 5).



Thank you for completing your product selection you are now being passed to our Secure Account Set Up area to complete the Account Set Up Process.

You will automatically move to the next section if nothing happens please click here

Рис. 5 Процес замовлення

Для отримання пробного сертифікату спочатку потрібно зареєструватися на сайті заповнивши реєстраційну форму. При заповненні інформації користувача слід вводити ім'я та прізвище латинкою (Рис. 6). Дозволяється заповнювати лише "необхідні" поля.

Certificate Applica	ation
1. Account Setup	2. Product Details 3. Completed
Account Details 🚿 Conf	irm Details

Account Details

Please specify details for your account. Your account contact will receive notices regarding your Certificate application and will be the main contact associated with your GlobalSign Certificate Center (GCC) account. If you are applying on behalf of someone else, enter their details, and you can specify an additional Technical Contact for yourself later in the application process.

User Information		
First Name Required	Vasyl	
Middle Name or Initial		
Last Name Required	Ivanov	
Email Address Required	ivanov.vasyl@gmail.com Please check email is accurate, this email address will be used in the application process	

Рис. 6 Форма. Інформація про користувача

Нижче наведено приклад заповнення інформації про організацію (Рис. 7). Її також слід заповнювати латинкою.

Primary Organization Details		
Organization Name Required	OA Specify the Organization Registered Name in full, including Inc, Ltd, NV, PIc etc Enter "Personal" if this Certificate is for personal use	
Department		
Street Address 1 Required	Seminarska, 2 e.g. Two International Drive	
Street Address 2	e.g. Suite 330	
City Required	Ostroh	
State / County Required	Ukraine	
Zip / Postal Code	35800	
Country Required	Ukraine - UA	
Phone Number Required	380365430258 e.g. 603-570-7060 or 01622 766766	
Fax Number	e.g. 603-570-7059 or 01622 662255	
Business Directory ID / Number	DUNs (D&B) Number If you have a Business Directory ID or Number (such as a DUNs number) please enter it here	
Organization Category	Select Business type	
Your TimeZone	GMT+02:00 Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	

Do you wish to register a trading address?

No O Yes

Рис. 7 Інформація про організацію

Після заповнення блоку "Деталі логіну" слід натиснути кнопку "Next" (Рис. 8). В якості "Username" найкраще вибрати ваше ім'я та прізвище латинкою без крапки та без пробілу. Дозволяється використовувати лише символи латинського алфавіту чи цифри. Мінімальна довжина "username" – 8 символів. Ті ж вимоги стосуються й пароля. Пароль слід ввести двічі однаковий.

GlobalSign Certificate Center (GCC) Login Details

Your GCC account allows you to manage all your GlobalSign Certificates and provides fast access to ordering additional products and renewing, reissuing and revoking current Certificates. Please create a memorable Username and Password.

Username Required	ivanowasyl Username is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)	
Password Required	Password is case sensitive and must be 8 - 64 characters. Alpha-numeric values only (A-Z, 0-9)	
Password(re-enter) Required	•••••	



Рис. 8 Деталі логіну

На наступній сторінці слід уважно перевірити введену на попередньому кроці інформацію, прочитати умови надання сервісу, погодитися з ними та натиснути кнопку "Next" (Рис. 9)



Рис. 9 Фрагмент умов надання сервісу

Наступний крок дозволяє задіяти додаткові можливості досвідченим користувачам, проте користувачі цієї інструкції до таких не належать, тому слід просто натиснувши кнопку "Next" перейти до наступного кроку (Рис. 10).



Product Details - Personal Sign 30 Day Demo

I have an externally generated CSR Check only if you are an Advanced User and have an externally generated Certificate Signing Request (CSR) Otherwise click Next	Yes, I have an externally generated CSR (advanced users only)
PKC S12 Option This option will create the public and private key on behalf of the subscriber. This is an alternative to the key generation taking place in the Subscriber's browser later in the application process.	Yes, use PKCS#12 Option
TOTAL COST (inc. Tax)	\$0



Рис. 10 Деталі продукту

Наступний крок дозволяє вказати яка mail-адреса буде використовуватися для ідентифікації сертифіката. Найпростіше використати електрону адресу вказану на одному з попередніх кроків. Зручно буде також використати пароль вказаний на одному з попередніх кроків. Пароль вказаний на цьому кроці буде використано для того, щоб "забрати" новостворений сертифікат (Рис. 11).



Certificate Identity Details

These details will be vetted and included as the certified identity within your issued Certificate. Make sure the details entered are correct - we will vet the details you include. To assist you, some details will be pre-populated from previous pages or from your GCC account details, you may overwrite these if needed.

Email Address Required	ivanov.vasyl@gmail.com	
	The specified email will be visible within the issued Certificield	cate in the Common Name

Create Temporary Pickup Password

Please create a temporary pickup password. You will only need this during the installation process. This is not the same as your account password.

If you forget this password you will need to resubmit your order. Please copy it somewhere safe.

Pickup Password Required	•••••	
	Password must be a minimum of 8 characters. Alpha-nume	eric values only (A-Z, 0-9)
Pickup Password (re-enter) Required	•••••]

Рис. 11 Деталі ідентифікації сертифіката

Крім того доведеться заповнити невеличку анкету (невеличка плата за безплатність ;)). Приклад заповнення анкети зображено нижче (Рис. 12).

How did you hear about Global Sign? Required	Referred by friend or Coworkers Referred by Microsoft Outlook/Website Researched Search Engine Researched Search Engine Advertisement (Side Advertisement) Informed by Advertisement/Campaign/Others I am a n exiting Customer/Partner I am a n exiting Test Cert User
Please specify the number of employees within your Organization. Required	1-10 employees 11-100 employees 101+ employees
Please specify your purpose for trialing a Personal Sign certificate. Required	For Demonstration/Test to your Client To evaluate if PersonalSign works for our Services/Products For Personal Use To evaluate PersonalSign for my Organization/Team
What do you intended using this test certificate for? Required	To Test Email Encryption To Test Digital Signature on Email To Test Authentication to secure network or devices To Test Digital Signature on Document Others (Free writing)
On completion of your 30 days trial do you plan to upgrade to a full Personal Sign certificate? Required	Yes, I will be purchasing a full certificate from GlobalSign Yes, I will be purchasing but unsure from which provider Yes, I will be purchasing multiple certificates No, I will be applying for another demo certificate No, I will be applying for another demo certificate No, I was for test purposes only
What factors would influence your decision to buy a digital certificate? Required	Support Sales/Relationship Cholce/Function/Option Issuance Speed Ease of Business Price Design of Website Preferred Service Provider
Who is your current certificate provider? Required	GlobalSign Verisign Thawte Comodo None/Others (Free writing)

Please complete the below questions to help us understand your digital certificate requirements

Рис. 12 Приклад заповнення анкети

Після заповнення анкети слід підтвердити, що пароль, який використовуватиметься для отримання сертифікату було збережено в надійному місці натиснути кнопку "Next" (Рис. 13).

Req	have copied this	password to a safe location
8	Back	Next D
	Рис. 13 Збережен	ня пароля у безпечному місці

На етапі "Підтвердження Деталей" (Рис. 14), слід лише погодитися з угодою і натиснути кнопку "Next" (Рис. 15).





Рис. 16 Завершення процесу реєстрації

Наступний етап — перевірка електронної пошти. Якщо все було зроблено правильно, то згодом на електронну пошту прийде три листи (Рис. 17).

🗋 🖈 🕞 approval	Order ID PC201210088011 GlobalSign PersonalSign 1 <test> - Ar</test>
по_герну	PC201210088011: Personal Sign 30 Day Demo Order Received for
🗌 📩 🛑 no_reply	Welcome to GlobalSign - Please note that this e-mail is automatic:

Рис. 17 Перших три листа від Globalsign

Лист який був отриманий останній слід відкрити і використати для підтвердження введеної на першому етапі інформації. Для цього слід скористатися посиланням, що розміщене у листі (Рис. 18).

Dear Customer,

An application for a PersonalSign 1 <Test> Certificate has been placed with GlobalSign for <u>ivanov.vasyl@gmail.com</u> (-) and Order ID PC201210088011.

In order for GlobalSign to issue the Certificate, the email address must be validated. Please follow the below link to choose to APPROVE or NOT APPROVE the application.

Only if you approve the application will the Certificate be issued.

https://regist.globalsign.com/ra/arrivalMailApproval/arrivalMailApproval/ ArrivalMailApproval.do?r=8791bb86&e=600e84f89855&c= 0a57da559db84478d2ffe53ed274fbfb00a2f58a

Рис. 18 Фрагмент листа з посиланням підтвердження

Після того як буде здійснено перехід за посиланням відобразиться сторінка підтвердження справжності електронної скриньки, на якій слід натиснути кнопку "APPRUVE" (Рис. 19).

APPROVE or DO NOT APPROVE Certificate Application

An application for a PersonalSign 1 <Test> Certificate for ivanov.vasyl@gmail.com (-) has been received.

In order to issue the Certificate, the right of the applicant to apply for the Certificate must be validated.

The following Applicant details were submitted during the ordering process. Please review the Applicant details below, and then:

Click I APPROVE to authorize the order, or;
 Click I DO NOT APPROVE to reject the order, the Certificate WILL NOT be issued.

Application Details	
Order ID	PC201210088011
Common Name	ivanov.vasyl@gmail.com
Contact First Name	Vasyl
Contact Middle Name	-
Contact Last Name	lvanov
Contact Phone	380365430258
Contact Email	ivanov.vasyl@gmail.com
Organization (O)	-
Locality (L)	-
State (S)	-
Country (C)	-
Application Email	ivanov.vasyl@gmail.com
Application Date	2012-10-08 20:16:04.351
IAPPRO	I DO NOT APPROVE

Рис. 19 Підтвердження інформації

Після підтвердження електронної скриньки слід знову перевірити електронну пошту. Повинен надійти ще один лист (Рис. 20).

	no_reply	Certificate Download Ready - PC201210088011: PersonalSign 30 Day Demc
	approval	Order ID PC201210088011 GlobalSign PersonalSign 1 <test> - Approve App</test>
	no_reply	PC201210088011: PersonalSign 30 Day Demo Order Received for ivanov.va
🗆 ☆ 📄	no_reply	Welcome to Global Sign - Please note that this e-mail is automatically sent

Рис. 20 Лист для завантаження сертифікату

Відкривши лист слід скористатися посиланням для завантаження сертифікату (Рис. 21).

HOW TO PICK UP & INSTALL YOUR CERTIFICATE

IMPORTANT:

For assistance please visit the appropriate support site:

Code Signing Certificate Support Site: <u>https://www.qlobalsign.com/support/codesign.php</u> PersonalSign Certificate Support Site: <u>https://www.qlobalsign.com/support/personalsign.php</u>

You must complete this process on the machine from which you intend to use the Certificate.

* Windows 2000 & XP Users: We recommend you use the Internet Explorer or Firefox browsers.

* Windows Vista Users: We recommend you do NOT use Internet Explorer. Please use Firefox (available free of charge from <u>www.mozilla.com</u>) to complete the process. If you have to use Internet Explorer, please click on the link below for detailed instructions on preparing the browser: www.globalsign.com/support/keygen/microsoft.php

Click on the link below to initiate the Certificate generation and installation process.

https://system.globalsign.com/pc/public/certificate/install.do?p= 8beb3e5f504286d25892dbfce33bb41aadf7bc3f

Make sure the above link is unbroken and complete. Copy and Paste the entire link into your browser if necessary.

Рис. 21 Фрагмент листа із посиланням для завантаження сертифікату

Після переходу за посиланням з'явиться можливість встановити сертифікат. Для цього потрібно ввести пароль, призначений для отримання сертифікату (він був створений Вами на одному з попередніх етапів) та натиснути кнопку "Next" (Рис. 22)

Install Certificate

You will now go through the Certificate generation and installation process. Note that if you continue on this computer, your Certificate will be installed on this computer.

Step One: Enter your Pickup Password

Your Pickup Password will have been set by the applicant during the application.

Enter the Pickup Password to continue.

Forgotten the Pickup Password? Click Here for instructions.



Рис. 22 Встановлення сертифікату

Вибір провайдера криптографічного сервісу (Рис. 23). Після погодження необхідних моментів натисніть кнопку "Next".

Install Certificate

Step Two: Select the Cryptographic Service Provider (CSP)

The CSP is used to generate the cryptographic keys within your Certificate. We have listed the CSPs found on your computer. For further assistance on using CSPs and which may be appropriate if you are installing your Certificate onto a hardware device such as crypto USB, view the CSP Support Guide.

Please note! Depending on your browser / Operating System setup, there may be a information bar or Pop Up asking you to install "Microsoft Certificate Enrolment Control" displayed at the top of this page. If so, you MUST allow this to run. It is a safe program that your browser uses to install your certificate. To run it, click on the information bar or Pop Up and follow the instructions.

Cryptographic Service Provider 2048 (Високий рівень) 💌	
GlobalSign Subscriber Agreement for PersonalSign Certificates Version 1.3	-
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANISATION. BY USING THE DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED DIGITAL CERTIFICATE OR CANCEL THE ORDER WITHIN 7 DAYS OF ISSUANCE TO GLOBALSIGN FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS AGREEMENT, E-MAIL US AT legal@globasign.com	-
This GlobalSign PersonalSign Subscriber Agreement ("Agreement") is effective as of the	
AGREE TO THE SUBSCRIBER AGREEMENT	

Please click Next and wait. Do not click Next again and do not close the browser, the process may take a few seconds.



Рис. 23 Вибір провайдера криптографічного сервісу

Наступне вікно дозволить встановити два сертифікати (Рис. 24):

- 1. Ваш особистий сертифікат (він буде розміщений у сховищі сертифікатів Google Chrome) (Рис. 25).
- 2. Сертифікат проміжного центру сертифікації (він буде необхідний для організації ланцюжка довіри і його слід зберегти на змінний носій) (Рис. 26).



Експорт сертифікату у файл

Для здійснення експорту сертифікату у файл слід пройти таку послідовність крокі на комп'ютері на якому було здійснено встановлення сертифікату:

1. Перейти до налаштувань Google Chrome

ublic/certificate/install.do		☆ 🗐
2, успішно збережено. Перегл	Нова вкладка Нове вікно Нове анонімне вікно Закладки	a Ctrl+N Ctrl+Shift+N
	Редагувати	Вирізати Копіювати Вставити
	Збільшити	- 100% +
Intermediate CA Certificates Istall My Certificate button to install the Ce	Зберегти сторінку як Знайти Друк Інструменти	Ctrl+S Ctrl+F Ctrl+P
	Історія Завантаження	Ctrl+H Ctrl+J
e detected that you are not using Internet ow the below instructions to install your C Install My Certificate button to install your C	Ви ввійшли як kotsyuk@g Налаштування 6 Про Google Chrome	mail.com
Install My Certficate	Переглянути фонові стор Довідка	інки (18)
below buttons to install the Intermediate C ensure that your Certificate will be trusted by yo	Вийти ur computer, and by others.	
Install CA Certficate1 🔹		

Рис. 27 Вхід у налаштування Google Chrome

2. Внизу сторінки знайти розширені налаштування



3. Перейти до підрозділу HTPS/SSL, та скористатися кнопкою "Керувати сертифікатами"

HTTPS/SSL



Рис. 29 Розділ HTTPS/SSL

4. Вибрати власний сертифікат та натиснути кнопку "Експорт..."

Сертифікати					
Призначення: <pre></pre>					
Особисті Інші користувач	ні Проміжні центри серти	ифікації Довір	оені кореневі центри	1 ▲ →	
Власник	Видавець	Термін дії	Зрозуміле ім'я		
ivanov.vasyl@gmai	GlobalSign PersonalSi	07.11.2012	<Немає>		
raaraa	GiobalSign PersonalSi raaraa	25.08.2110	<memae> <hemae></hemae></memae>		
Імпорт Експорт Призначення сертифіката	Видалити		Додат	ГКОВО	
Локладніше про сертифікат	ги		Перегля	яд	
			Закр	ити	

Рис. 30 Діалогове вікно "Сертифікати"

5. Запуск майстра сертифікатів, слід натиснути кнопку "Далі".



6. Експортування закритого ключа, слід вибрати можливість "Так" та натиснути кнопку "Далі"

Майстер експорту сертифікатів	x
Експортування закритого ключа Можна експортувати закритий ключ разом із сертифікатом.	
Закриті ключі захищено паролем. Щоб експортувати закритий ключ разом із сертифікатом, необхідно ввести пароль у наступних діалогових вікнах. Експортувати закритий ключ разом із сертифікатом?	
 ні, не експортувати закритий ключ 	
докладнше про <u>експортування закритих ключів</u>	
< Назад Далі > Скасу	вати

Рис. 31 Експортування закритого ключа

7. Формат експорту. Використайте можливість додати всі сертифікати до шляху сертифікації. Решту прапорців не варто ставити.

Майстер експорту сертифікатів
Формат файлу експорту Сертифікати можна експортувати у файли різних форматів.
Виберіть формат, який слід використовувати:
🔘 Файл в DER-кодуванні X.509 (.CER)
🔘 Файл в Base64-кодуванні X.509 (.CER)
🔘 Стандарт Cryptographic Message Syntax – сертифікати РКСЅ #7 (.Р7В)
За можливості додати всі сертифікати до шляху сертифікації
обміну особистими відомостями – РКСЅ #12 (.PFX) в можливості додати всі сертифікати до шляху сертифікації
Видалити закритий ключ після успішного експортування
Експортувати всі розширені властивості
🔘 Сховище серіалізованих сертифікатів Microsoft (.SST)
Докладніше про <u>формати файлів сертифікатів</u>
< Назад Далі > Скасувати

Рис. 32 Формат експорту

8. Захист приватного ключа паролем. Використайте той самий пароль, який використовували протягом генерації сертифікату. Пароль слід ввести двічі однаковий.

Майстер експорту сертифікатів	x
Пароль Задля підтримки безпеки необхідно захистити закритий ключ паролем.	
Введіть і підтвердьте пароль. Пароль: Введіть і підтвердьте пароль (обов'язково):	
< Н <u>а</u> зад Да <u>л</u> і > Скасува	ати

Рис. 33 Захист приватного ключа паролем

9. Скористайтеся кнопкою "Огляд..." для вказання місця розташування та імені файлу експорту.

Файл для експорту	TWO IS IN THE REAL PROPERTY OF	
Укажіть ім'я файлу, з	який слід експортувати	
Ім'я файлу:		
1		Огляд

Рис. 34 Ім'я та розташування файлу експорту

10. Назва файлу експорту. Виберіть розташування файлу таким чином, щоб його легко було знайти (наприклад створіть на змінному носію папку keys\global) давши йому ім'я згідно зразка. Після виконання вимог натисніть кнопку "Зберегти".

			-
ги 🔻 Створити п	апку	844	
эння таження	Бібліотека "Д] Упорядкування за: Пап	ка 💌
но <mark>в</mark> ідвідане іий стіл	E IM'8	~	
e Drive	Πο	шук не дав результатів.	
ки			
projekt_10-06-22			
e Drive			
nts_to_download			
osti			
аписи	- (III		
файлу: ivanov.vasyl.	global.privat		

Рис. 35 Назва файлу та розташування

11. Після вказання шляху до файлу експорту слід натиснути кнопку "Далі"

стер експорту сертифіка	атів
Файл для експорту Укажіть ім'я файлу, як	кий слід експортувати
<u>І</u> м'я файлу:	
E:\DOC\keys\global\iv	vanov.vasyl.global.privat.pfx

Рис. 36 Шлях до файлу експорту

12. Завершення роботи майстра – натисніть кнопку "Готово".

Майстер експорту сертифікатів	the second s	X	
	Завершення роботи майстра експорту сертифікатів Майстер експорту сертифікатів успішно завершив роботу. Указані такі параметри:		
	Ім'я файлу Ключі експорту Подати всі сертифікати во швоху сертифікації	Так	
	Формат файлу	Φai	
	•	Þ	
	< Назад Готово Сн	касувати	

Рис. 37 Завершення роботи майстра

Після повідомлення про успішний експорт закрийте модальне вікно та діалогове вікно "Сертифікати".

Перевірте чи дійсно вдалося експортувати файл. За вказаним Вами шляхом повинен бути приблизно

🔽 🌛 ivanov.vasyl.global.privat.pfx 🚽

такий файл:

Імпорт сертифіката від Globalsign

Здійснення імпорту сертифікату від Globalsign в Internet Explorer

Сертифікат від Globalsign дозволяє здійснювати операцію підписування документів MS Office. Для того, щоб реалізувати цю можливість потрібно в операційній системі встановити власне сам сертифікат. Встановити сертифікат можливо з допомогою операції імпорту. Для імпорту сертифікату в Internet Explorer слід просто зробити подвійний клік на файлі експорту

🔽 🏂 ivanov.vasyl.global.privat.pfx

Подальший процес імпорту описаний у вигляді сукупності ілюстрованих кроків¹:

Майстер імпорту сертифікатів	Вас вітає майстер імпорту сертифікатів Цей майстер допомагає копіювати сертифікати, списки довірених сертифікатів та списки відкликаних сертифікатів із диска до сховища сертифікації, підтверджує особу користувача та містить відомості, потрібні для захисту даних або встановлення захищених мережних підключень. Сховище сертифікатів – ще системна область, у якій зоерігаються сертифікати. Щоб продовжити, натисніть кнопку "Далі".
	< Н <u>а</u> зад Да <u>л</u> і > Скасувати

1. Запуск майстра імпорту сертифікатів (Рис. 38).

Рис. 38 Стартове вікно майстра імпорту сертифікатів

¹ В залежності від операційної системи та її версії послідовність кроків майстра може дещо відрізнятися.

2. Вказання файлу для здійснення імпорту (Рис. 39). Насправді файл вказувати не потрібно, так як він був вибраний автоматично в момент подвійного кліка на файлі.

Майстер імпорту сертифікатів
Файл для імпорту Укажіть файл, який потрібно імпортувати.
Iм'я файлу: \\yaa \DOC \keys\global\\vanov.vasyl.global.privat.pfx
Примітка. Кілька сертифікатів може зберігатися в одному файлі в таких форматах:
Файл обміну особистими відомостями – РКСЅ #12 (.PFX,.P12)
Стандарт Сгуртодгарпіс Message Syntax – сертифікати РКСS #7 (.Р7В) Сховище серіалізованих сертифікатів Microsoft (.SST)
Докладніше про <u>формати файлів сертифікатів</u>
< Назад Далі > Скасувати

Рис. 39 Вказання імені файлу

- 3. Ввід пароля таємного ключа (Рис. 40).
 - а. Для здійснення імпорту слід ввести пароль доступу до таємного ключа.
 - b. Встановити прапорець «Увімкнути сильний захист закритого ключа». Це дасть можливість навіть на публічному комп'ютері здійснювати підпис, при цьому, під час кожного використання закритого ключа буде запитано пароль доступу до нього.
 - с. Встановити прапорець «Позначити цей ключ як придатний до експорту». Це дасть можливість і надалі здійснювати операції імпорту з допомогою цього ж файлу.

Майстер імпорту сертифікатів
Пароль Задля підтримки безпеки закриті ключі захищено паролями.
Введіть пароль для закритого ключа. а Пароль:
 Вімкнути сильний захист закритого ключа. Якщо ввімкнути цей параметр, щоразу під час використання застосунком закритого ключа буде з'являтися запит. с Позначити цей ключ як придатний до експорту. Це дозволить архівувати або передавати ключі пізніше.
🔲 Долучити всі розширені властивості.
Докладніше про <u>захист закритих ключів</u>
< Н <u>а</u> зад Да <u>л</u> і > Скасувати

Рис. 40 Майстер імпорту ввід пароля таємного ключа

4. Вибір сховища сертифікатів. На цьому кроці слід скористатися функцією автоматичного вибору сховища на основі типу сертифікату (Рис. 41).

Майстер імпорту сертифікатів	x
Сховище сертифікатів Сховища сертифікатів – це області системи, в яких зберігаються сертифікати.	
Можна визначити місце для сертифіката вручну або дозволити це зробити системі Windows.	
<u>ибирати сховище сертифіката на основі типу сертифіката автоматичної</u> <u>Р</u> озташовувати всі сертифікати в такому сховищі	
Сховище сертифікатів: 	
Докладніше про <u>сховища сертифікатів</u>	
	вати

Рис. 41 Сховище сертифікатів

5. Завершальний крок налаштування майстра (Рис. 42).

<u>s</u>	Завершення роботи майстра імпорту сертифікатів Сертифікат буде імпортовано після натискання кнопки "Готово". Указані такі параметри:	
	Вибране сховище сертифікатів Вміст Ім'я файлу	Автоматично визнача PFX \\raa\DOC\keys\global
	. m	×
	< Назад	отово Скасувати

Рис. 42 Завершення налаштування майстра

6. Початкове вікно імпорту сертифікату в Internet Explorer (Рис. 43). Слід вибрати високий рівень безпеки.

	Sacrocynok cit	зорює захи	щении елем	ент.
	Закритий ключ (CryptoAPI		
	Установлено се рівень безпеки	редній	становити р	івень безпеки
1	∕становлено се зівень безпеки	редній	(становити р	івень безп

Рис. 43 Початкове вікно імпорту

7. Вибрати високий рівень безпеки (Рис. 44).

Вибір рівня безпеки	
	Оберіть відповідний рівень безпеки для цього елемента. Вимагати дозвіл і пароль у разі використання цього елемента. Середній Вимагати дозвіл у разі використання цього елемента.
	< Назад Далі > Скасувати

Рис. 44 Вибір рівня безпеки

8. Захист таємного ключа паролем (Рис. 45). На цьому етапі можна встановити інший пароль для доступу до таємного ключа, проте, рекомендується ввести такий же як і на попередніх кроках, щоб не заплутатися. Пароль слід ввести двічі однаковий, щоб система змогла переконатися, що Ви не зробили помилки під час вводу його першого разу.

Створити пароль для захисту цього елемента.
Створити новий пароль для цього елемента. Пароль для: Закритий ключ CryptoAF
Пароль:
< Назад Готово Скасувати

Рис. 45 Створення пароля таємного ключа

9. Підтвердження імпорту (Рис. 46).



Рис. 46 Підтвердження імпорту ключа

10. Повідомлення про успішний імпорт 🙂 (Рис. 47).



Рис. 47 Повідомлення про успішний імпорт

Тепер на комп'ютері, на якому щойно було здійснено імпорт сертифікату можна виконати <u>підпис</u> <u>документа MS Word</u>.

Здійснення імпорту сертифікату від Globalsign в The Bat

Для того, щоб здійснити імпорт експортованого сертифікату від Globalsign слід завантажити поштовий клієнт The Bat з налаштованою скринькою та виконати низку ілюстрованих кроків, наведених нижче.

- 1. Відкрийте властивості скриньки (Рис. 48).
 - а. Виберіть свою власну скриньку, якщо їх більше ніж одна, як показано на рисунку.
 - b. Відкрийте меню «Скринька».
 - с. Виберіть підпункт «Властивості».



Рис. 48 Властивості скриньки
- 2. Відкрити можливість редагувати сертифікати (Рис. 49).
 - а. Виберіть розділ «Загальні відомості».
 - b. Натисніть кнопку «Редагувати сертифікати».

☐ Зберегти лист Девізи Звук Листування Нотатки	
--	--

Рис. 49 Властивості скриньки, Загальні відомості

- 3. Розпочати процес імпорту (Рис. 50).
 - а. Переконайтеся, що відкрита вкладка сертифікат.
 - b. У переліку сертифікатів можуть існувати попередні сертифікати. Так на рисунку такий сертифікат існує. Це сертифікат, який Іванов Василь згенерував собі сам. Разом з тим такого сертифікату може не існувати (якщо одне з попередніх завдань виконано не було).

c.	Натиснути	кнопку «Імпортування»

		Застарі	є Кореневий
ванов Василь	Іванов Василь	28.10.20	013 Іванов Вас.
Імпортування	Перегляд	Створити	Скинути підписи

Рис. 50 vCard, вкладка "Сертифікати"

- 4. Вибір файлу експорту для здійснення імпорту (Рис. 51).
 - a. Вкажіть шлях до файлу з якого будете здійснювати імпорт. (Якщо експорт здійснювався у паку ..\keys\global, то саме до неї слід вказати шлях).
 - b. Виберіть файл у який Ви експортували сертифікат від Globalsign.
 - с. Переконайтеся, що у полі «Ім'я файлу» вибрано потрібний файл.
 - d. Натисніть кнопку «Відкрити».

ипортування сертифікатів із файсія	×
Core keys ► global	👻 😽 🗍 Пошук: global 🖇
Упорядкувати • Створити папку	II • 🔟 🔞
IM'S	Дата змінення Ти
b 🛛 🖓 ivanov.vasyl.globa	al.privat.pfx 09.10.2012 1:16 Φa
c • •	III .
Ім'я файлу ivanov.vasyl.global.privat.pfx	• Bci файли (*.*) •
	d <u>В</u> ідкрити 🔻 Скасувати

Рис. 51 Вибір файлу для імпорту

5. Введіть пароль для розшифрування особистого ключа та натисніть кнопку «Так» (Рис. 52)

🗰 Вкажіть РFX парол	
Вкажіть пароль для ре ivanov.vasyl.global.priv	озшифрування особистого ключа, збереженого в rat.pfx.
EN	Так Скасувати Допомога

Рис. 52 Ввід пароля для розшифрування закритого ключа

6. Повторно введіть пароль для розшифрування особистого ключа та натисніть кнопку «Так» (Рис. 53).



Рис. 53 Повторний ввід пароля

7. В результаті імпорту з'явиться від одного до трьох сертифікатів. Слід зробити подвійний клік на Вашому сертифікаті від Globalsign, щоб перевірити його справжність (Рис. 54).

vCard-файл - ACCOUNT.VC Загальні Особисте Робоч	СF - Іванов Василь е Сертифікати Інш	e			
Для кого випущений	Ким випущений		Застаріє		Кореневий
ivanov.vasyl@gmail.com GlobalSign Root CA GlobalSign PersonalSign	Іванов Василь GlobalSign Perso GlobalSign Root 1 GlobalSign Root	onalSign 1 CA CA CA	28.10.2013 07.11.2012 28.01.2028 13.04.2019	20:54:02 12:00:00 10:00:00	Іванов Bac GlobalSign GlobalSign GlobalSign
Імпортування Експортування	<u>П</u> ерегляд Видалення	Створити 		Скин Редак	ути підписи тор пристрою
	ongenetitiv	201011		Гедик	rop npherpolo

Рис. 54 Перегляд нового сертифікату

- 8. Слід перевірити дійсність сертифікату (Рис. 55).
 - а. Якщо піктограма сертифікату має зелений кружок з прапорцем й існує напис «Цей сертифікат є дійсним», можна одразу натиснути кнопку «Так» і перейти до кроку № 10. Якщо ж сертифікат недійсний:
 - b. Слід перейти у вкладку «Шлях».

Сертифікат		X
вагальні Деталі Шлях		
(mg)		
Сертифікатна інформація		
цей сертифікат є дисним		
Bat! може використовувати и вати и ва На вати и вати ват	цей сертифікат для: шифрування повідомлення - так,	
перевірка цифрового підпису по	відомлення - так, TLS з'єднання - ні.	
Для кого випущений:	ivanov.vasyl@gmail.com	
Ким випущений:	GlobalSign PersonalSign 1 CA - G2	
Дійсний з 08.10.2012 20:54:02 µ	10 07.11.2012 20:54:02	
Ви маєте особистий ключ, що	відповідає цьому сертифікату.	
Додати до адресної книги	Так	-

Рис. 55 Перевірка дійсності сертифіката

- 9. Додайте сертифікат до довірчих (Рис. 56).
 - а. Виберіть кореневий сертифікат.
 - b. Натисніть кнопку «Додати до Довірчих (Trusted)».
 - с. Після цього натисніть кнопку «Так».

Загальні Деталі Шлях	
Шлях сертифіката	
GlobalSign Root CA	
ivanov.vasyl@gmail.com	
b	
Додати до Довірчих (Trusted)	Перегляд
Статус сертифіката	
Цей сертифікат є дійсним	
	_
	c

Рис. 56 Ланцюжок сертифікатів

10. Натисніть кнопку «Скинути підписи…» (Рис. 57). Це потрібно для вибору потрібного сертифікату при наступному доступі до таємного ключа. Якщо цього не зробити, то автоматично буде використано попередній ключ. Якщо Ви бажаєте кожен раз під час підписування документів використовувати інший ключ, цю операцію потрібно буде повторювати постійно.

💘 vCard-файл - ACCOUNT.VCF - I	ванов Василь		×
Загальні Особисте Робоче С	ертифікати Інше		
Для кого випущений	Ким випущений	Застаріє	Кореневий
🚰 Іванов Василь	Іванов Василь	28.10.2013	Іванов Вас
ivanov.vasyl@gmail.com	GlobalSign PersonalSign 1 C	A 07.11.2012 20:54:02	GlobalSign
📑 GlobalSign Root CA	GlobalSign Root CA	28.01.2028 12:00:00	GlobalSign
📑 GlobalSign PersonalSign 1	GlobalSign Root CA	13.04.2019 10:00:00	GlobalSign
Імпортування	Перегляд Стве	орити Скин	нути підписи
Експортування Е	Видалення <u>З</u> а	пит Редан	стор пристрою
		Так Відміна	Допомога

Рис. 57 Скидання підписів

11. Підтвердіть операцію скидання підписів, натиснувши «ОК».

Card-фай	л - ACCOUNT.VCF - Іванов Василь
?	Кожна з ваших особистих адрес електронної пошти повинна мати сертифікат підпису за замовчуванням. Ви можете мати кілька сертифікатів, які містять ті самі електронні адреси. При виконанні наступної операції підписування вас буде запитано, який з ваших сертифікатів слід використовувати для підписування листів, які надсилаються з вказаної адреси.
	ОК Скасувати

Рис. 58 Підтвердження операції скидання підписів

12. Підтвердіть виконані дії натиснувши кнопку «Так» (Рис. 59).

агальні Особисте Робоче	Сертифікати Інше		
Для кого випущений	Ким випущений	Застаріє	Кореневий
🎽 Іванов Василь 🎽 ivanov.vasyl@gmail.com 🜁 GlobalSign Root CA 🜁 GlobalSign PersonalSign 1	Іванов Василь GlobalSign PersonalSign 1 CA GlobalSign Root CA GlobalSign Root CA	28.10.2013 07.11.2012 20:54:02 28.01.2028 12:00:00 13.04.2019 10:00:00	Іванов Bac GlobalSign GlobalSign GlobalSign

Рис. 59 Діалогове вікно "Сертифікати"

13. Підтвердіть виконані дії натиснувши кнопку «Так» (Рис. 60).

 Загальні відомості Транспорт Спеціальне Установки 	<u>Н</u> азва Ів	анов на gmail		
 Установки Файли і каталоги Шаблони 	Інформація відправі	Редагувати сер ника	гифікати	<u>Р</u> едагувати vCard
Новий лист Відповідь Переадресація Підтвердження проч	Ім'я <u>в</u> ідправника <u>А</u> дреса відправника <u>О</u> рганізація	Іванов Василь ivanov.vasyl@g	gmail.com	
Девізи Эвук Девізи Эвук Листування Нотатки	Зворотна інформац Зворотне <u>і</u> м'я <u>З</u> воротна адреса	iя (Reply-To)		
	Адресна книга за за 🔲 Використовуват Шаблон імені вірту	мовчуванням: ти <u>ц</u> ю скриньку уальної папки:	<за замовчув для посилань [%Name]	танням> ▼
t H				

Рис. 60 Підтвердження імпорту та налаштувань

Використання сертифікату від Globalsign для накладання електронного цифрового підпису в документах MS Word

Перш ніж виконувати накладання цифрового підпису в документі MS Word, слід здійснити <u>імпорт</u> <u>сертифікату в Internet Explorer</u>.

Накладати підпис можна на документ який вже названий та збережений. Тому, перш ніж розпочати процедуру підписування, слід створити документ MS Word та зберегти його з певною назвою. Пропонується дати таку назву документа: «Прізвище Ім'я підпис» де замість Прізвища та Імені вставити своє прізвище та ім'я¹.

Підпис документів MS Word 2013

1. Відкрийте підготований документ MS Word у текстовому процесорі MS Word (Рис. 61).

	l	- 0 X
Solution → Solutio	🕶 🍫 Пошук: globa	al 👂
Упорядкувати 🔻 Включити до бібліотек	ки • » 🔢	• 🔟 🔞
Г Ім'я	Дата змінення	Тип
🧔 ivanov.vasyl.global.privat.pfx	09,10,2012 1:16	Файл обміну п
🔯 Іванов Василь підпис.docx	19.10.2012 8:57	Microsoft Word
* [•

Рис. 61 Документ MS Word у папці

¹ В залежності від операційної системи та її версії процес підписування документа MS Office може дещо відрізнятися.

2. Перейдіть у меню FILE (Рис. 62).



Рис. 62 Документ MS Word перед накладанням підпису

3. У розділі «Info» відкрийте великою кнопкою «Protect Document» випадаюче меню та виберіть пункт «Add a Digital Signature» (Рис. 63).



Рис. 63 Розділ "Info"

- 4. Вибір підпису¹ (Рис. 64).
 - а. Вкажіть тип відповідальності.
 - b. Вкажіть причину підписування.
 - с. Натисніть кнопку «Change...» для того, щоб вибрати серед існуючих підписів свій.

Sign	? ×
See additional information about what you are signing	
You are about to add a digital signature to this document. This signature to this document.	ire will not be
Created this document	
Purpose for signing this document: Навчальна мета	
b o include information about the signer, click the details button.	Details
Signing as: ivanov.vasyl@gmail.com Issued by: GlobalSign PersonalSign 1 CA - G2	Change
Sign	Cancel

Рис. 64 Діалогове вікно "Підпис"

¹ Перш ніж виконувати накладання цифрового підпису в документі MS Word, слід здійснити <u>імпорт сертифікату</u> <u>в Internet Explorer</u>.

5. Виберіть свій підпис та натисніть кнопку «ОК» (Рис. 65).



Рис. 65 Вибір сертифікату

6. Натисніть кнопку «Sign», для накладання підпису (Рис. 66).

Sign	? ×
6 See additional information about what you are signing	
You are about to add a digital signature to this document. This si visible within the content of this document.	gnature will not be
<u>C</u> ommitment Type:	
Created this document	
Purpose for signing this document:	
Навчальна мета	
To include information about the signer, click the details butto	n. <u>D</u> etails
Signing as: ivanov.vasyl@gmail.com	Change
Issued by: GlobalSign PersonalSign 1 CA - G2	<u>cn</u> ange
Sign	Cancel

Рис. 66 Накладання підпису

7. Надайте дозвіл на використання таємного ключа та підтвердіть свій вибір паролем (Рис. 67).



Рис. 67 Пароль доступу до закритого ключа

8. У повідомленні про успішне накладання підпису просто натисніть «ОК» (Рис. 68).



Рис. 68 Підтвердження успішності накладання підпису

9. В результаті операції підписування з'явиться позначка «Signed Document» (Рис. 69). Для перегляду підпису слід клацнути кнопку «View Signatures».



Рис. 69 Позначка про підпис документа

10. На завершальному рисунку показано як можна переглянути підпис (Рис. 70).

📲 🖯 5 - С 🖄 - 🗁 А - 📼 🚿 🗅 🥰 💽 АРА 🗟 📴 - » Іванов Ві	асиль підп ? 🗵 🗕 🗖 🗙
FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW	VIEW ADD-INS ABBY 🕨 🙂
MARKED AS FINAL An author has marked this document as final to discourage editing. Edit Anyway	×
Спробуйте-змінити-текст-не-вруйнувавши-цифровий-підпис-;)¶	Signatures Valid signatures: ivano 19.10.2012 This document is signed. Any edits made to this document will invalidate the digital signatures. Learn more about signatures it Office documents
PAGE 1 OF 1 8 WORDS UKRAINIAN	- + 117%

Рис. 70 Перегляд підпису

Підпис документів MS Word 2010

1. Відкрийте підготований документ MS Word у текстовому процесорі MS Word (Рис. 71).

		- • • *
G v ↓ « keys ► global ·	🗕 😽 Пошук: globi	al 👂
Упорядкувати 🔻 Включити до бібліотен	«и ▼ » 🔠	• 🔟 🔞
Г Ім'я	Дата змінення	Тип
ivanov.vasyl.global.privat.pfx	09,10,2012 1:16	Файл обміну п
🔯 Іванов Василь підпис.docx	19.10.2012 8:57	Microsoft Word
· · · · · · · · · · · · · · · · · · ·		+

Рис. 71 Документ MS Word у папці

2. Перейдіть у меню «Файл» для накладання електронного цифрового підпису (Рис. 72).





3. У розділі «**Відомості**» скористайтеся кнопкою «**Установити захист**» та виберіть можливість «**Додати цифровий підпис**» (Рис. 73).

Jukpana		Цей продукт потрібно	Властивості *	
ідомості		активувати	Розмір	0 байт
		Продукт Microsoft Office	Сторінки	1
станні	Активувати продукт	потребує лійсної ліцензії для	Слова	8
		продукту. Щоб отримати дійсну	Загальний час редагування	2 хв
творити		ліцензію для продукту, активуйте	Заголовок	Додати на
		ключ продукту зараз.	Теги	Додати тег
рук			Примітки	Додати ко
		Дозволи	Пов'язані дати	
берегти та надіслати		Усі можуть відкривати, копіювати	Дата змінення	Ніколи
opinea	Установити	та змінювати будь-яку частину цього документа.	Створено	Сьогодні, 2
obititio	захист *		Надруковано	Ніколи
] Параметри	Позначити як ос	таточний	100 S. 1 S. 1	
Вихід	Позначення док	умента як остаточного та призначеного	Пов'язані користувачі	
	лише для читанн	19.	Автор	Юрій Коцюк
	🛄 Шифрувати пар	олем		Додати авт
	Для відкриття ць	ого документа необхідний пароль.	Востаннє змінено	Ще не збе…
	<u>О</u> бмежити реда	гування	Deferrent en muneur	
	Керування типал	ии змін, які можуть вносити користувачі до	. Word 97-2003 скор	истайтеся поси
	цього документа		ord.odf¶	
	Обмежити дозві	л за користувачем	and the second s	
	Надання доступу можливості реда	[,] користувачам з одночасним позбавленням агування, копіювання та друку.	50	
	Додати цифров	ий підпис		
	Забезпечення ці	лісності документа за допомогою	alCignum angenes interes	

Рис. 73 Меню додавання цифрового підпису

4. Встановіть причину підпису та натисніть кнопку «**Змінення…**», для того, щоб вибрати серед існуючих сертифікатів свій¹ (Рис. 74).

ідпис	and in the local division of the local divis	
Див. додать	ові відомості про те, що ви підписуєте	ĥ
Ви збираєтеся дод невидимим у вміст <u>М</u> ета підписання ц Навчальна мета	ати цифровий підпис до цього документ і цього документа. њого документа:	а. Цей підпис буде
Підписання як: Постачальник:	ivanov.vasyl@gmail.com GlobalSign PersonalSign 1 CA - G2	<u>З</u> мінення
		Ідпис Скасувати

Рис. 74 Встановлення причини підпису

5. Серед існуючих сертифікатів виберіть свій сертифікат від Globalsign та натисніть кнопку «**ОК**» (Рис. 75).

Безпека Window	s X
Вибір серт	ифіката
	ivanov.vasyl@gmail.com Постачальник: GlobalSign Personal Дійсний з: 08.10.2012 до 07.11.2012 Щоб переглянути властивості се)
	kotsyuk@gmail.com Постачальник: GlobalSign Personal Дійсний з: 08.10.2012 до 07.11.2012
	raaraa Постачальник: гаагаа Дійсний з: 25.02.2011 до 01.02.2111
	ОК Скасувати

Рис. 75 Перелік існуючих сертифікатів

¹ Перш ніж виконувати накладання ^{цифрового} підпису в документі MS Word, слід здійснити <u>імпорт сертифікату в</u> Internet Explorer.

6. Натисніть кнопку «Підпис» для початку процесу накладання Вашого підпису (Рис. 76).

Тідпис		2 ×
Див. додати	ові відомості про те, що ви підписуєте	20 14
Ви збираєтеся дод невидимим у вміст <u>М</u> ета підписання L	(ати цифровий підпис до цього документ і цього документа. цього документа:	ra. Цей підпис буде
Навчальна мета		
Підписання як: Постачальник:	ivanov.vasyl@gmail.com GlobalSign PersonalSign 1 CA - G2	<u>З</u> мінення
		јідпис Скасувати

Рис. 76 Підпис

7. Надайте дозвіл на використання таємного ключа та підтвердіть свій вибір паролем (Рис. 77).

Запит дозволу на використання	ключа
Дозволити або заборонити	и застосунку використовувати ключ
Ім'я ключа:	Зазначене у застосунку ім'я ключа • Надати дозвіл • Відмовити в дозволі
Пароль захисту ключа:	*****
😧 Переглянути відомості про кл	пюч ОК Скасувати

Рис. 77 Пароль доступу до закритого ключа

8. У повідомленні про успішне накладання підпису просто натисніть «ОК» (Рис. 78).



Рис. 78 Підтвердження успішності накладання підпису

9. В результаті операції підписування з'явиться позначка «Підписаний документ» (Рис. 79). Для перегляду підпису слід клацнути кнопку «Перегляд підписів».



Рис. 79 Ініціація перегляду підпису

10. На завершальному рисунку показано як можна переглянути підпис (Рис. 80).

👿 🗔 🤊 - 🕐 - 🔄 А 🚍 🖌 🗋 🎒 🖓 Сост 🔊 🕬 🦓 📿	ав ^і (ОД ання	обового вано □ □ × Видяд Надбудови АБВҮҮ Translation ♡ 3
Позначено як остаточний Автор позначив цей документ як остаточний, щоб заг	побігти	в у Редагувати Х
L	Br	дписи • *
		💭 Припустимі підписи:
		ivanov.vasyl@gmail.com 25.10.2012
Спробуйте-змінити-текст-не-зруйнувавши-цифрови	1	
- 1		
N -		
- m -		
· · ·		
	- I	Цей документ підписано.
	* E	удь-які зміни, внесені в документ, зроблять ифрові підписи недійсними.
	Ŧ	Додаткові відомості про підписи в документах Office
Сторінка: 1 з 1 Слів: 8 🍼 українська 鼠 🛅] 🛃 📃 124% 🝚 🛛 🔶

Рис. 80 Перегляд підпису

Підпис документів MS Word 97-2003

Для довідки щодо підпису документів MS Word 97-2003 скористайтеся посиланням: <u>http://www.acsk.uss.gov.ua/download/manual/MSWord.pdf</u>, або ж виконайте послідовність кроків у вигляді графічних зображень¹.

1. Відкрийте заздалегідь підготований документ MS Word (Рис. 81).

Відкриття док	уме нта								? 🗙
Папка:	📙 global			~	🊱 - 🔰	🔍 👌	< 📸 🏢	• Сервіс •	
	🖭 Іванов Вас	иль підпис							
Мої останні документи									
робочий стіл									
Мої документи									
Г Мій комп'ютер									
	Ім'я файлу:	1					~		Piacoutu
Моє мережне оточення	Тип файлів:	' Усі докумен'	ги Word				~		Скасувати

Рис. 81 Відкриття документа для підпису

¹ Увага, в залежності від версії операційної системи чи версії MS Office послідовність кроків може незначно відрізнятися

2. Скористайтеся меню «Сервіс», та виберіть підменю «Параметри» (Рис. 82).

🔄 Іванов Василь підпис - Microsoft Word						
<u>: Ф</u> айл ∏равка Вигл <u>я</u> д Вст <u>а</u> вка Фор <u>м</u> ат	Сервіс Таблиця Вікно Довідка Введіть запитання 🗸 🗙					
i 🗅 💕 🔒 👌 🖨 🖪 🐧 🖤 📖 🖿	🕰 Правопи <u>с</u> F7 🚦 Times New Roman 👻					
L	🔣 Довідкові матеріали АІІ+Клацнути					
	Мова на					
N	Виправити пошкоджений текст					
1	Статистика					
-	省 Автореферат					
-	Спіл <u>ь</u> на робоча область					
• Це підписаний документ	Bunpaвлення Ctrl+Shift+E					
-	Порівняти й об'єднати документи					
1	Установити захист					
N	Спільна ро <u>б</u> ота •					
1	<u>Л</u> исти й розсилки •					
m -						
4	Шаблони та надбудови					
-	🤫 Парам <u>е</u> три автозаміни					
<u>د</u>	настройка					
-	Параметри					
Стор. 1 Розд 1 1/1 На 2,5см	Рд 1 Кол 23 ЗАП ВИПР ВДЛ ЗАМ українська 🔐 🏢					

Рис. 82 Відкриття меню "Параметри"

3. У діалоговому вікні «Параметри» виберіть вкладку «Безпека», і натисніть кнопку «Цифрові підписи…» (Рис. 83).



Рис. 83 Доступ до кнопки "Цифрові підписи..."

4. Для того, щоб додати Ваш підпис до цифрових підписів документа у діалоговому вікні «**Цифровий підпис**» вкладки «**Підписи**» натисніть кнопку «**Додати…**» (Рис. 84).

Цифровий підпис		
Підписи		
Створений в Office ц легальний підпис. Д підписи в довідці.	ифровий підпис може не утв ив. додаткові відомості про	зорювати цифрові
Цифрові підписи док	умента:	
Підписано	Цифровий підпис вид	Дата
Пр <u>и</u> єднувати сер Перегляд сертифік Довідка	тифікати до доданих підпис ката	ів <u>В</u> идалити
	OK	Скасувати

Рис. 84 Додавання цифрового підпису

5. У діалоговому вікні «Select Certificate» виберіть власний сертифікат¹ та натисніть кнопку «**ОК**» (Рис. 85).

Select Certificate		? 🛛
Select the certificate you wa	ant to use.	
Issued to	Issued by	Expiration Date
ivanov.vasyl@gmail	GlobalSign PersonalSig	07.11.2012
<	Ш	>
ſ	OK Cancel	<u>V</u> iew Certificate

Рис. 85 Вибір сертифікату

¹ Якщо серед переліку сертифікатів Вашого сертифікату немає, Вам потрібно повторно <u>здійснити імпорт</u> <u>сертифікату в Internet Explorer</u>.

6. У наступному діалоговому вікні слід ввести пароль, яким було захищено Ваш приватний ключ на етапі імпорту та натиснути кнопку «OK». Не слід ставити прапорець «Remember password», інакше накладати підпис від Вашого імені зможе будь-хто, хто працюватиме за цим же комп'ютером.

Signing data	Signing data with your private exchange key 🛛 🛛 🔀				
	An application is requesting access to a Protected item. CryptoAPI Private Key				
М.	OK Cancel <u>D</u> etails				

Рис. 86 Підпис даних Вашим приватним ключем

7. Для того щоб накласти підпис натисніть кнопку «ОК» (Рис. 87).

Цифровий підпис		×
Підписи		
Створений в Office ц легальний підпис. Ді підписи в довідці.	ифровий підпис може не утворювати ив. додаткові відомості про цифрові	
Цифрові підписи док	умента:	
Підписано	Цифровий підпис вид Дата	1
🔛 ivanov.vasyl	GlobalSign PersonalSign 28.10.2012	
✓ Пр <u>и</u> єднувати сер Перегляд сертифік Довідка	тифікати до доданих підписів ата <u>Д</u> одати <u>В</u> идалити	
	ОК Скасува	яти

Рис. 87 Цифровий підпис

8. Для того щоб закрити діалогове вікно «Параметри» натисніть кнопку «ОК» (Рис. 88).

Параметри ? 🔀					
Правопис Виправлення Користувач Сумісність Розташування Вигляд Загальні Правка Друк Збереження Безпека					
Параметри шифрування для цього документа пароль для відкриття файлу:					
Параметри спільного використання для цього документа паро <u>л</u> ь дозволу запису:					
рекомендувати доступ лише для <u>ч</u> итання Цифрові підписи Установити за <u>х</u> ист					
Параметри захисту конфіденційної інформації					
попереджувати перед друком, збереженням і надсиланням файлу, який містить записані виправлення та примітки зберегти випадкове число для підвищення точності злиття					
✓ показувати приховану розмітку при відкритті та збереженні Захист від макросів					
Змінювати рівень безпеки при відкритті файлів, які можуть містити віруси в макросах, і вказувати надійних розробників макросів.					
ОК Скасувати					

Рис. 88 Діалогове вікно "Параметри"

9. Дійсний електронний цифровий підпис буде відображено на інформаційній панелі підписаного документа MS Word (Рис. 89). Для того, щоб перевірити справжність сертифікату зробіть на ньому підвійний клік.

🕲 le	📲 Іванов Василь підпис - Microsoft Word													
: <u>Ф</u> а	йл	Правка	Вигл <u>я</u> д	Вст <u>а</u> вка	Фор <u>м</u> ат	С <u>е</u> рвіс	<u>Т</u> аблиця	<u>В</u> ікно	<u>До</u> відка	В	ведіть з	апитання		• ×
: D	2	🖬 🔒	88	ABC	ii b	<u>- (* 5</u>	😫 🗉	100%	- 🕜	🕮 <u>Ч</u> итання	T i 🔋	imes New	Roman	
	٠Ā	• • • 1 •	1 • 2 • 1	3 • 1 • 4	5	6 . 1 . 7	• 1 • 8 • 1	· 9 · 1	· 10 · I · 11	• • • 12 • • • 1	3 • • • 14	‡• I • 15 <u>∕</u>	1 + 16 +	- ~
~														=
-														
-														
•	т	To minn			-									
-	T	це пъдп	исании	докумен	r.									
-														
+														
?														
4														
1														~
БО														±
7														•
د ≣ ⊑		5 Q <												>
Стор	o. 1	Роз	д 1	1/1	На 2,5см	Рд 1	Кол 23	ЗАП	випр вдл	ЗАМ укра	інська	₿ 2	8	

Рис. 89 Значок відображення цифрового підпису

10. Для перегляду сертифікату у діалоговому вікні «**Цифровий підпис**» виберіть сертифікат, який потрібно перевірити та натисніть кнопку «**Перегляд сертифікати…**» (Рис. 90).

Цифровий підпис				
Підписи				
Створений в Office цифровий підпис може не утворювати легальний підпис. Див. додаткові відомості про цифрові підписи в довідці.				
Цифрові підписи док	умента:			
Підписано	Цифровий підпис вид Дата			
🔤 ivanov. vasyl	GlobalSign PersonalSign 28.10.2012			
Приєднувати серт Перегляд сертифік Довідка	гифікати до доданих підписів ата Додати Видалити			
	ОК Скасувати			

Рис. 90 Перегляд сертифікату

11. У вкладці «General» діалогового вікна «Certificate» можна проглянути загальну інформацію про сертифікат, а перейшовши у вкладку «Certification Path» — переглянути повний шлях сертифікації та справжність сертифікатів (Рис. 91).

Certificate ?X
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s): •Proves your identity to a remote computer •Protects e-mail messages •1.3.6.1.4.1.4146.1.40
* Refer to the certification authority's statement for details.
Issued to: ivanov.vasyl@gmail.com
Issued by: GlobalSign PersonalSign 1 CA - G2
Valid from 08.10.2012 to 07.11.2012
$\ref{eq: relation}$ You have a private key that corresponds to this certificate.
Issuer Statement
ОК

Рис. 91 Загальна інформація про сертифікат

12. Після перевірки справжності сертифікату натисніть кнопку «ОК» (Рис. 92).

Certificate	? 🛛
General Details Certification Path Certification path GlobalSign GlobalSign PersonalSign 1 CA - G2 Vanov.vasyl@gmail.com	
Certificate <u>s</u> tatus: This certificate is OK.	View Certificate

Рис. 92 Вкладка "Шлях сертифікації"

Використання сертифікату від Globalsign для надсилання підписаних, зашифрованих, підписаних/зашифрованих листів з допомогою The Bat

Підписування листів сертифікатом від Globalsign

Для підписання листа у The Bat з використанням сертифікату від Globalsign слід виконати низку ілюстрованих кроків¹:

1. Скористайтеся кнопкою на кнопочній панелі інструментів для надсилання листа, або ж меню Лист/Створити (Рис. 93).

😚 The Bat!			
<u>Л</u> ист Спеціальне <u>П</u> апка	<u>С</u> кринька <u>І</u> нстр	ументи П <u>е</u> регляд <u>О</u> пці	ї Допомога 鱳
Назва	Непроч	нита Всього	
🗄 👩 kotsyuk at gmail	1	2	
🖃 🛅 Іванов на gmail			- Pourse
🖄 Вхідні		0	
- 😭 Вихідні		0	🖂 🖻 🛈 🏳 Від Кому Тем
— 🕞 Надіслані		0	
- Кошик		0	
📑 Вхідні - відомі		0	
Усі / Непрочитані / Адре	си /		Усі Непрочитанные С флажком
			📆 Звичайний текст
	-		

Рис. 93 Кнопка надсилання листа

¹ Для реалізації накладання підпису потрібно <u>імпортувати у The Bat сертифікат з особистим ключем від</u> <u>Globalsign</u>

2. Для того, щоб накласти електронний цифровий підпис слід в меню «Конфіденційність» активувати можливість «Дозволити S/MIME» та «Підписати по закінченню» (Рис. 94).

Редагування повідомлення	
Дист Редагувати Пошук Формат Утиліти Перевірка орфограф	й Конфіденційність Перегляд Опції Зашифоквати по закінченню Опцаписати по закінченню Дозволити OpenPGP Встановити стандартно Захист РGP/MIME • • • • • • • • • • • • •

Рис. 94 Накладання підпису

- 3. Вкажіть одержувача ¹ повідомлення, тему, як вказано на рисунку та, власне, тіло повідомлення (Рис. 95).
 - а. Ще раз перевірте чи накладатиметься у Вас підпис.
 - b. Після перевірки натисніть кнопку «**Розмістити повідомлення у вихідних**», це дасть можливість ще раз перевірити підпис перед відправкою.

🛞 Редагуванн	ня повідомлення -> Юрій Коцюк <kotsyuk@gmail.com></kotsyuk@gmail.com>
ј b едагу	увати <u>П</u> ошук <u>Ф</u> ормат <u>У</u> тиліти Пере <u>в</u> ірка орфографії <u>К</u> онфіденційність П <u>е</u> регляд <u>О</u> пції 🧱
Від:	Іванов Василь <ivanov.vasyl@gmail.com></ivanov.vasyl@gmail.com>
Кому:	Юрій Коцюк <kotsyuk@gmail.com></kotsyuk@gmail.com>
Копія:	
Тема:	Підписаний лист від GlobalSign
● ● ■	
Janui Ja	ист підписано із анкористанням сертифікату від GlobalSign. mailto:kotsyuk@gmail.com
2:69	Вставка 📗 🐺 🐺 🏀 English (American) 🝙 😔 🤯 kotsyuk at gmail 🚯 <u>Т</u> екст (MicroEd)

Рис. 95 Вказання одержувача

¹ В якості одержувача виберіть одногрупника/партнера, який також надішле Вам підписаний лист. Рекомендується вибрати більше ніж одного партнера. Якщо партнера вибрати не вдається слід звернутися за допомогою до старости групи.
4. Серед існуючих ключів виберіть ключ від Globalsign¹ (Рис. 96) та натисніть кнопку «Так».

силь n PersonalSign 1 CA	28.10.2013	Іванов Василь
n PersonalSign 1 CA	07 11 20	
	07.11.20	

Рис. 96 Вибір сертифікату для підпису

5. Введіть пароль доступу до приватного ключа від Globalsign, та натисніть кнопку «Так» (Рис. 97)

Вхідни	ій пароль S/MIME			
Вкажіть r ivanov.va	тароль для розшифрува syl@gmail.com.	ння особистого	ключа сертифіката S/	/MIME для
1				
EN	Перегада	Так	Скасувати	Лопомога

Рис. 97 Пароль приватного ключа від Globalsign

¹ Якщо у Вас більше одного сертифікату, то перед цією операцією слід виконати операцію <u>скидання підписів</u>.

- 6. У папці «Вихідні» з'явиться готовий до відправки лист (Рис. 98).
 - а. Перейдіть у папку «Вихідні».
 - b. Виберіть підписаний лист.
 - с. Натисніть кнопку «**Переглянути ДІЙСНІ підписи**», щоб переконатися, що саме Ваш підпис накладено¹.

Haana	Hernewers	Pereze	1	
	пепрочита	БСБОГО		i 🞧 • 🖄 • 📝 • 🖄 • 🖄 💆 🖄 📠 🐼 🚽
± kotsyuk at gmail	1	2	100	
Іванов на gmail		1		
а 🛃 Вхідні		0		
🔡 Вихідні		1		🖾 🕅 🟳 Від Кому Тема
Надіслані		0	h	🧏 🔹 🔹 Іванов Василь Юрій Коцюк Підписаний лист від Glob
- Кошик		0		
				< III Усі / Непрочитанные / С флажком /
				Усі / Непрочитанные / С флажком / Від: Іванов Василь <ivanov.vasyl@gmail.com> Кому: Юрій Коцюк <kotsyuk@gmail.com> Тема: Підписаний лист від GlobalSign</kotsyuk@gmail.com></ivanov.vasyl@gmail.com>
				Ш Усі Непрочитанные С флажком Від: Іванов Василь <ivanov.vasyl@gmail.com> Кому: Юрій Коцюк <kotsyuk@gmail.com> Тема: Підписаний лист від GlobalSign Доброго дня Юрій, С</kotsyuk@gmail.com></ivanov.vasyl@gmail.com>
			200 H	 Т Усі Непрочитанные С флажком Віді: Іванов Василь Віда: Іванов Василь Кому: Юрій Коцюк С Доброго дня Юрій, Даний лист підписаний з використанням сертифікату від GlobalSign
			200 H	 Усі Непрочитанные С флажком Від: Іванов Василь <ivanov.vasyl@gmail.com> Кому: Юрій Коцюк <kotsyuk@gmail.com> Тема: Підписаний лист від GlobalSign</kotsyuk@gmail.com></ivanov.vasyl@gmail.com> Доброго дня Юрій, Даний лист підписаний з використанням сертифікату від GlobalSign

Рис. 98 Перевірка наявності підпису

¹ Якщо кнопки підпису немає, значить з якоїсь причини Вам не вдалося накласти підпис. Спробуйте повторити все з початку.

7. Переконайтеся, що використовується потрібний підпис та натисніть кнопку «Так» (Рис. 99).

Перегляд цифрово	го підпису		
Цей лист перевірено у	спішно. Правильні підписи детальн	о вказані нижче.	
Статус	Час підписання	Для кого випущений	Ким випущений
Так	24.10.2012 22:30:04	ivanov.vasyl@gmail.c	GlobalSign PersonalS
Перегляд			Так

Рис. 99 Перегляд цифрового підпису

Шифрування листів із використанням сертифікату від Globalsign

Для здійснення шифрування листів із використанням сертифікату від Globalsign необхідно перш за все здійснити імпорт відповідного відритого ключа в адресну книгу The Bat. Це можна здійснити кількома шляхами:

- 1. Безпосередній імпорт з використанням файлу експорту відкритого ключа.
- 2. Використання підписаного з використанням Globalsign одногрупником¹ листа для здійснення операції імпорту в адресну книгу.

Так як перший спосіб використовувався в одному з попередніх завдань у даному прикладі буде продемонстрований другий спосіб, коли респонденти не можуть обмінятися ключами особисто.

¹ В якості одержувача виберіть одногрупника/партнера, який також надішле Вам підписаний лист. Рекомендується вибрати більше ніж одного партнера. Якщо партнера вибрати не вдається слід звернутися за допомогою до старости групи.

Імпорт ключа в адресну книгу

1. Ініціюйте перевірку пошти на своїй поштовій скриньці (Рис. 100).

Лист Спеціальне Папка С	кринька <u>І</u> нструменти П <u>е</u> регляд <u>О</u> пції	Допомога 🎆
Назва	Непрочита Всього	
∃ 🏠 kotsyuk at gmail	1 3	
🔁 Вхідні	1 2	kotsvuk at omail
😭 Вихідні	0	Іванов на gmail
🕞 Надіслані	1	🛛 👝 👘 Іванов на gmail (Тема <
- 🔤 Кошик	0	Гарания в скриг
— 🔛 Вхідні - відомі	0	👖 🛄 Надіслатин і Геревірити для всіх Коцюк 🏾 The Bat! 7
🗄 🛅 Іванов на gmail	1	
Вхідні	0	
📸 Вихідні	1	
🕞 Надіслані	0	
- Т Кошик	0	
🛃 Вхідні - відомі	U	Big: RITLABS <th.bat@ritlabs.com> Komy: Kopii Koupor <kotsyuk@gmail.com> Tema: The Bat!</kotsyuk@gmail.com></th.bat@ritlabs.com>
		Welcome to The Bat!
		Once you have installed The Bat!, you receive at your disposal not just an ordinary email client. The Bat! is something greater. It will facilitate your routine work, lessening the time you spend daily for your correspondence. It will adjust

Рис. 100 Перевірка пошти

2. Введіть пароль доступу до своєї поштової скриньки та натисніть «Так» (Рис. 101).

Задача	Перебіг	Лист	Очікува	Пройшло	Переда	симв/сек	Запис
🦫 🔹 Іванов н	a 0%	0/?		00:00:56			
	🕌 Іванов	s на gmail	- перевірка	пошти		×	
Сервер:	Ім'я ко	ристувача:	1				
	Пароль	vasyi@gma	n.com				
Статус	•••••	••••••					
	Пон	овити дан	і поштової ск	риньки			
			Так		Скасувати		
Час	h						
		112		12	1	-	- 1)

Рис. 101 Ввід пароля до поштової скриньки

3. Вкажіть потрібний лист в обробнику листів та натисніть кнопку «Обробити пошту» (Рис. 102).

😽 Іван	ов н	a gmail - O	бробник л	истів						
<u>Л</u> ист	Виб	і <u>р Г</u> лобал	њні <u>П</u> ерег	гляд						
		2 🗳		۲ 🔮	*					
	#	Прочитані	Прийняти	Видалити	Відкрити	Розмір	Від	Кому	Тема	Час
	15	2				<mark>6 840</mark>	Юрій Коцюк <k< td=""><td>ivanov.va</td><td>Підписаний GlobalSign л</td><td>20:22:24</td></k<>	ivanov.va	Підписаний GlobalSign л	20:22:24
*										•

Рис. 102 Обробник листів

4. Відкривши у папці «Вхідні» отриманий лист, скористайтеся відповідною кнопкою, щоб перевірити підпис (Рис. 103).

🐼 The Bat!	State Association and	
<u>Л</u> ист Спеціальне <u>П</u> апка <u>С</u>	кринька Інструменти П <u>е</u> регляд <u>О</u> пці	ї Допомога 🇱
Назва	Непрочита Всього	
🗉 👩 kotsyuk at gmail	1 3	
— 🚰 Вхідні — 🎯 Вихідні	1 2 0	🔁 🛃 🖆 🍄 🎽 💽 Пошук
— 🕞 Надіслані	1	🖂 🖻 🔟 🖾 Від Кому Тема 😽
- 📷 Кошик	0	🦉 🔹 Юрій Коцюк ivanov.vasyl@gm Підписаний GlobalSign лис
— 🚰 Вхідні - відомі	0	
Геанов на gmail Генерание в страние в стр	2	
	1	
	0	4 III
Вхідні - відомі	0	Усі / Непрочитанные / С флажком /
		Від: Юрій Коцюк <kotsyuk@gmail.com> Кому: ivanov.vasyl@gmail.com Тема: Підписаний GlobalSign лис</kotsyuk@gmail.com>
		Доброго дня ivanov,
		З поєвгою, Ropiù mailto:kotsyuk@qmail.com
Усі Непрочитані Адресі	1/	
😭 Іванов на gmail 24.10.	2012, 20:47:11: FETCH - з'єднання заверше	но - отримано 1 листів 🤀 Звичайний текст

Рис. 103 Відкриття підписаного листа

5. Зробіть подвійний клік на підписі для того, щоб перевірити його та додати до адресної книги (Рис. 104).

💓 Перегляд цифрового пі,	дпису		
Цей лист перевірено успіш	но. Правильні підписи детально) вказані нижче.	
Статус	Час підписання	Для кого випущений	Ким випущений
📑 Так	24.10.2012 20:22:29	kotsyuk@gmail.com	GlobalSign PersonalS
Перегляд			Так

Рис. 104 Перегляд цифрового сертифікату

6. Додайте сертифікат до адресної книги та натисніть кнопку «Так» (Рис. 105). Якщо ж сертифікат не дійсний, слід перейти у вкладку «Шлях» та додати ланцюжок сертифікатів до довірчих.



Рис. 105 Сертифікатна інформація

7. Щоб додати ланцюжок сертифікатів до довірчих, виберіть сертифікат кореневого центру сертифікації та натисніть кнопку «Додати до довірчих (Trusted)» (Рис. 106), після цього натисніть кнопку «Так».

Сертифікат	X
Загальні Деталі Шлях	
Шлях сертифіката	
GlobalSign Root CA GlobalSign PersonalSign 1 CA - G2	
Додати до Довірчих (Trusted)	Перегляд
татус сертифіката	
Цей сертифікат є дійсним	
	Так

Рис. 106 Шлях сертифікації

8. Закінчіть перегляд сертифікату, натиснувши «Так» (Рис. 107).

💓 Перегляд цифрового і	підпису		
Цей лист перевірено успі	шно. Правильні підписи детально	о вказані нижче.	
Статус	Час підписання	Для кого випущений	Ким випущений
📑 Так	24.10.2012 20:22:29	kotsyuk@gmail.com	GlobalSign PersonalS
<u>П</u> ерегляд			Так

Рис. 107 Перегляд цифрового сертифікату

Надсилання зашифрованого листа

1. Викличте форму для надсилання листа натиснувши потрібну кнопку (Рис. 108).

The Bat!		221 223	
<u>Л</u> ист Спеціальне <u>П</u> апка	<u>Скринька</u> Інструм	ленти П <u>е</u> регляд <u>О</u> пь	ії Допомога 🎇
Назва	Непрочи	та Всього	
∃ 👩 kotsyuk at gmail	1	2	
🗄 🛅 Іванов на gmail			
🔂 Вхідні		0	Паралини Санана С
📑 Вихідні		0	🖾 🖻 🗍 🗜 Від Кому Тема
— 🕞 Надіслані		0	aby and the fit light light light light light
- 📷 Кошик		0	
🔄 🚰 Вхідні - відомі		0	
			И И И И И И И И И И И И И И И И И И И
Усі / Непрочитані / Адре	си		
			🖫 Звичайний текст

Рис. 108 Кнопка надсилання листа

 Вкажіть адресу одержувача, тему повідомлення, та власне напишіть тіло повідомлення. Скористайтеся меню «Конфіденційність», для того щоб перевірити чи стоїть прапорець «Дозволити S/MIME», та активуйте можливість «Зашифрувати по закінченню» як вказано на рисунку нижче (Рис. 109).

💛 Редагувани	ня повідомлення -> Юрій Коцюк <kotsyuk@gmail.com></kotsyuk@gmail.com>	Col Name	
Лист Редаг	увати <u>П</u> ошук <u>Ф</u> ормат <u>У</u> тиліти Пере <u>в</u> ірка орфографі	<u>К</u> онфіденційність Т <u>ерегляд О</u> пції 🎆	
a . 🖄	» o o d x n n d	🕲 Зашифрувати по закінченню	A A A
Від:	Iванов Василь ≺ivanov.vasvl@gmail.com>		
Кому:	Юрій Коцюк <kotsyuk@gmail.com></kotsyuk@gmail.com>		
Колія:		<u>В</u> становити стандартно	
Тема:	Зашифрований GlobalSign лист	Захист +	<u>```</u>
		DGD/MIME >	
Game R.		Voro vorimus	
ROBUNDEOG	ao amanina unianany itani, amanina no Raun ;)	were remark	
-			
	mailto:ivanov.vasyl@gmail.com		
			202
4:18	Вставка 📋 🛒 🚎 🧱 English (Ameri	can) 🔲 🤟 🦗 Іванов на gmail 💽 <u>Т</u> екст	(MicroEd)

Рис. 109 Підготовка до відправки зашифрованого листа

3. Після виконаних у пункті 2 дій натисніть кнопку «**Підготувати до відправки**» (Рис. 109, а). У Вас з'явиться можливість вказати який із сертифікатів отримувача буде використано для зашифровування. Виберіть сертифікат від Globalsign та натисніть кнопку «Так» (Рис. 110).

Виберіть сертифікат	B-		
иберіть сертифікат для шиф	фрування листів до kotsyuk@gmail.com	1	
Для кого випущений	Ким випущений	Застаріє	Кореневий ЦСК
🛃 kotsyuk@gmail.com	GlobalSign PersonalSign 1 CA	07.11.20	GlobalSign Root CA
■НОрій Коцюк	Юрій Коцюк	28.10.2013	Юрій Коцюк
Перегляд			Так Відміна

Рис. 110 Вибір сертифікату для шифрування листів

4. В результаті успішної операції шифрування у папці «Вихідні» з'явиться ще один лист. Якщо його вибрати, як показано на рисунку нижче (Рис. 111), то можна перевірити чи правильно його зашифровано, натиснувши на кнопку «Розшифрувати повідомлення S/MIME» (Рис. 111, а).

😽 The Bat!		-	
<u>Л</u> ист Спе <u>ц</u> іальне <u>П</u> апка <u>С</u> к	ринька <u>І</u> нструмен	ти П <u>е</u> регл	ляд <u>О</u> пції Допомога 🍔
Назва	Непрочита	. Всього	
🖻 👩 kotsyuk at gmail	1	4	
Вхідні Вихідні Надіслані Вхідні - відомі Вхідні - відомі Вхідні - відомі Вхідні - відомі Вхідні - відомі Вихідні С Вихідні С Вихідні	1	2 0 1 1 0 13 1 2 0	С С С С С С С С С С С С С С С С С С С
Вхідні - відомі		0 •	Усі Непрочитанные Сфлажком Від: Іванов Василь «ivanov.vasyl@gmail.com> Кому: kotsyuk@gmail.com Тема: Зашифрований GlobalSign лист Це повідомлення зашифровано S/MIME. Клацніть кнопку "Безпека" для його розшифрування/перевірки -870 6 Рагt.tx бай
Панов на gmail			😤 Звичайний текст
Conserves the grade			



5. В результаті перевірки система повідомить, що Ви не маєте права розшифрувати даний лист, натомість таке право має лише власник вказаного таємного ключа від Globalsign, тобто одержувач Вашого листа (Рис. 112). Тому просто натисніть кнопку «**Відміна**».

👸 Виберіть сертифікат	-		
Ви не маєте сертифіката, що бути розшифрованим одним	відповідає особистому ключу для роз з наступних одержувачів:	шифрування	і цього листа. Цей лист може
Для кого випущений	Ким випущений	Застаріє	Кореневий ЦСК
kotsyuk@gmail.com	GlobalSign PersonalSign 1 CA	07.11.20	GlobalSign Root CA
Перегляд			Так Відміна

Рис. 112 Невдала спроба розшифрувати лист без таємного ключа

Шифрування та накладання підпису із використанням сертифікату від Globalsign

Одночасне підписування та шифрування листа передбачає наявність усіх умов необхідних як для підписування так і для шифрування (див. <u>Підписування листів сертифікатом від Globalsign</u> та <u>Шифрування листів із використанням сертифікату від Globalsign</u>). Якщо ж усі умови виконуються то підписання та шифрування листа можна здійснити виконавши низку вказаних нижче ілюстрованих кроків.

1. Скористайтеся кнопкою «Нове повідомлення» для відкриття форми написання листа (Рис. 113).



Рис. 113 Кнопка "Нове повідомлення"

 Вкажіть адресу одержувача, тему повідомлення, та власне напишіть тіло повідомлення. Скористайтеся меню «Конфіденційність», для того щоб перевірити чи стоїть прапорець «Дозволити S/MIME», та активуйте можливість «Зашифрувати по закінченню» та «Підписати по закінченню» як вказано на рисунку нижче (Рис. 114).

У Редагування повідомлення -> kotsyuk@gmail.com <u>Лист</u> <u>Редагувати</u> <u>Пошук</u> <u>Ф</u> ормат <u>У</u> тиліти Перевірка орфографі М Ф ормат <u>У</u> тиліти Перевірка орфографі В В	Конфіденційність Перегляд <u>О</u> пції 🎉 Пацимфрувати по закінченню	
а Iванов Василь <ivanov.vasyl@gmail.com> Кому: kotsyuk@gmail.com Копія: </ivanov.vasyl@gmail.com>	Дозволити OpenPGP Дозволити S/MIME Встановити стандартно Захист рсв/МIME	
Асброго дня Юрій, Даний лист містить цифровий підпис, і яких прочитати текст, то Ви вдало його розшифрували. Поселом <u>mailto ivanov vasyl@gmail.com</u>	р Вам вдалося	
🗐 4:57 Вставка 🔲 🛒 🚎 📫 English (America	an) 🔲 🥪 🤯 Іванов на gmail 🚺 І	екст (MicroEd)

Рис. 114 Підготовка до відправки підписаного та зашифрованого листа

3. Після виконаних у пункті 2 дій натисніть кнопку «Підготувати до відправки» (Рис. 114, а). У наступному діалоговому вікні Вам буде надано можливість вибрати один з Ваших сертифікатів для підпису. Серед існуючих ключів виберіть ключ від Globalsign¹ (Рис. 115) та натисніть кнопку «Так».

¹ Якщо у Вас більше одного сертифікату, то перед цією операцією слід виконати операцію <u>скидання підписів</u>.

ія кого випущений	Ким випущений	Застаріє	Кореневий ЦСК
Іванов Василь	Іванов Василь	28 10 2013	Іванов Василь
ivanov.vasyl@gmail.com	GlobalSign PersonalSign 1 CA	07.11.20	GlobalSign Root CA

Рис. 115 Вибір сертифікату для підпису

4. Введіть пароль доступу до приватного ключа від Globalsign, та натисніть кнопку «**Так**» (Рис. 116)

HANNITE P			valous centudivers C	MIME and
anov.va	syl@gmail.com.	ння особистого	ююча сертифіката 5/	миме для

Рис. 116 Пароль для розшифрування особистого ключа

5. У наступному діалоговому вікні у Вас з'явиться можливість вказати який із сертифікатів отримувача буде використано для зашифровування. Виберіть сертифікат від Globalsign та натисніть кнопку «Так» (Рис. 117).

ля кого випущений	Ким випущений	Застаріє	Кореневий ЦСК
kotsyuk@gmail.com	GlobalSign PersonalSign 1 CA	07.11.20	GlobalSign Root CA
ыюри коцюк	юри коцюк	28.10.2013	юри коцюк

Рис. 117 Вибір сертифікату для шифрування листа

6. В результаті успішної операції шифрування у папці «Вихідні» з'явиться ще один лист. Якщо його вибрати, як показано на рисунку нижче (Рис. 118), то можна перевірити чи правильно його зашифровано та підписано, натиснувши на кнопку «Безпека повідомлення» (Рис. 118, а).

— — — — — Назва	Непрочи	та Всього			I CA C			
🗄 👩 kotsyuk at gmail	1	4		•	• 🕼 • 🖾	• 🕎 🔛 🖻	2 🛗 🖂 🖂 🦷	
— 🚰 Вхідні — 😭 Вихідні	1	2 0	ß	6	C [®] C [®] E	1 🗄 🖬	🚺 Пошук	
🕞 Надіслані		1		ŵВ	Rin	Kons	Taua	- Oto
- ТКошик		1	• 🔛	0 •	Іванов Василь	kotsyuk@gmail.co	m Зашифрофаний підписаний	i Glob 22:30
На видні - відомі		0	2	•	Іванов Василь	kotsyuk@gmail.co	m Зашифрований GlobalSign /	ист 22:11
ванов на дтан		14	. 199	÷.,	Іванов расиль	юрій коцюк	підписаний лист від Globals	ign 20:15
Видні		3						
🕞 Надіслані		0						
- 🗑 Кошик		10	•			III.		
🛃 Вхідні - відомі		0	Усі	Непроч	итанные 📈 С фл	ажком		a
				Від: Кому: Тема:	lванов Василь <iv kotsyuk@gmail.co Зашифрофаний г</iv 	anov.vasyl@gn m підписаний Glo	Розшифрувати повідомленн	a S/MIME
				Цеп	овідомлення з	ашифровано S/N	Переглянути ДІИСНИЙ серт	ифікат



7. Для перевірки яким сертифікатом було зашифровано лист виберіть можливість «Розшифрувати повідомлення S/MIME» (Рис. 118, б). В результаті перевірки система повідомить, що Ви не маєте права розшифрувати даний лист, натомість таке право має лише власник вказаного таємного ключа від Globalsign, тобто одержувач Вашого листа (Рис. 119). Тому просто натисніть кнопку «**Відміна**».

😸 Виберіть сертифікат	1		
Ви не маєте сертифіката, що в бути розшифрованим одним з	ідповідає особистому ключу для роз в наступних одержувачів:	шифрування	цього листа. Цей лист може
Для кого випущений	Ким випущений	Застаріє	Кореневий ЦСК
📧 kotsyuk@gmail.com	GlobalSign PersonalSign 1 CA	07.11.20	GlobalSign Root CA
<u>П</u> ерегляд			Так Відміна

Рис. 119 Невдала спроба розшифрувати лист без таємного ключа

 Для перевірки електронного цифрового підпису натисніть на кнопку «Безпека повідомлення» (Рис. 118, а) та виберіть можливість «Переглянути ДІЙСНІ підписи» щоб переконатися, що саме Ваш підпис накладено¹. (Рис. 118, в). Після перевірки натисніть кнопку «Так» (Рис. 120).

Цей лист перевірено успішно. Правильні підписи детально вказані нижче.					
Статус	Час підписання	Для кого випущений	Ким випущений		
🖪 Так	24.10.2012 22:30:04	ivanov.vasyl@gmail.c	GlobalSign PersonalS		

Рис. 120 Перегляд цифрового підпису

¹ Якщо кнопки підпису немає, або використано не той що слід підпис, значить з якоїсь причини Вам не вдалося накласти потрібний підпис. Спробуйте повторити все з початку.

Надсилання підготованих до відправки листів

1. Скористайтеся кнопкою для надсилання пошти, щоб надіслати свою пошту (Рис. 121).

лист спеціальне <u>П</u> апка <u>с</u> Іазва	кринька інстр Непро	нита. Всього	
🖗 kotowk at amail	1	A	
	1		kotowik at amail
ванов на дтан		14	🕞 Пошук (
Вхідні		1	
Вихідні			🖾 🖄 Надіслати листи з усіх скриньок 🛛 🖉 Тема
Надіслані		0	Надіслати+Перевірити для всіх
Кошик		10	т зашифровании GlobalSign лист 24
ы види відвий		1	
			Від: Іванов Василь ≺ivanov.vasyl@gmail.com> Кому: Юрій Коцюк ≺kotsyuk@gmail.com> Тема: Підписаний лист від GlobalSign
			Доброго дня Юрій,
			Даний лист підписаний з використанням сертифікату від GlobalSign — Э посвеою, Jeacos mailto ivanov vasyl@omail.com

Рис. 121 Відправка пошти

2. Введіть пароль доступу до Вашої поштової скриньки та натисніть кнопку «Так» (Рис. 122).

Задача	Перебіг	Лист	Очікува	Пройшло	Переда	симв/сек	Запис	
🖓 🔹 Іванов на	0%	0/3		00:00:14	0/18 614			
	🔀 Іванов	s на gmail -	надсилают	ься 3 листі	в	×		
Сервер: 0	Iм'я ко ivanov	ристувача: vasyl@gmail	.com					
Статус		овити дані і	тоштової ск	риньки				
Лист: Передавання:			Так		Скасувати			
Час: <u>Ж</u> урнал:	b		_	_				
надсилання пош Початок TLS-підт 5/N сертифіката: Зласник: US, Cali	ти - З листів вердження 3B74FF7B00 fornia, Mou	у черзі зв 100000068A8, ntain View, б	алгоритм: loogle Inc, s	RSA (1024 e mtp.gmail.e	бітів), випуш com.	цений 12.09	.2012 11	:57
2		Почтиния		Поцика		л	аталі	

Рис. 122 Ввід пароля доступу до поштової скриньки

3. Якщо листи вдалося відправити вони зникнуть з папки «Вихідні» та з'являться у папці «Надіслані» (Рис. 123).

🔂 The Bat!	the Analyzanian A	
<u>Л</u> ист Спе <u>ц</u> іальне <u>П</u> апка <u>С</u> крині Назва	ыка Інструменти Перегляд Непрочита Всього 1 4 14 1 0 3 10 0	Опції Допомога ∰
Усі Непрочитані Адреси	00-00-40, CEND	Не завантажено жодних повідомлень

Рис. 123 Папка "Надіслані"