Электронная цифровая подпись и импорт подписанных обменных файлов XML

Закона Согласно Украины землеустройстве (смотрите 0 http://zakon1.rada.gov.ua/laws/show/5394-17), идентифицировать для того, чтобы автора, подтвердить целостность и неизменность передаваемых обменных файлов XML, они должны быть подписаны электронной цифровой подписью. Электронная цифровая подпись — это специальные данные, которые добавляются в обменный файл XML. В результате этого, файл меняет расширение на .p7s и его нельзя будет изменить до тех пор, пока подпись не снимут (например, при проверке подписи). Если же кто-то подкорректировал этот файл, он не пройдёт проверку подписи, а подписать его может только владелец подписи.

Электронная цифровая подпись используется согласно *ДСТУ 4145-2002* (принят и введён в действие приказом государственного комитета Украины по вопросам технического регулирования и потребительской политики от 28 декабря 2002 года № 31). В данном стандарте использованы ссылки на следующие стандарты:

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая.

Алгоритм криптографического преобразования.

ГОСТ 34.311-95 Информационная технология. Криптографическая функция хеширования.

Более детально Закон Украины об электронной цифровой подписи читайте — <u>http://zakon4.rada.gov.ua/laws/show/852-15</u>

На данный момент, программа **GIS 6** (начиная с версии **6.1.7.6**) может автоматически подписывать экспортируемые обменные файлы, а также импортировать подписанные файлы, если подпись прошла проверку. Что для этого нужно?

1. Приобретаем электронный цифровой ключ

Это самое первое и главное требование. Без него Вы не сможете подписывать обменные файлы! *Компания ШЕЛС* не продаёт цифровые ключи для подписи. Для этих целей существуют специальные центры сертификации ключей (далее ЦСК). Вы можете найти тот ЦСК, который Вам больше подходит по цене и условиям, но уточняйте подойдёт ли данный ключ для землеустройства. Нами протестирован и поддерживается цифровой ключ ЦСК *«Украинские специальные системы»* (<u>http://csk.uss.gov.ua</u>).

В результате, Вам дадут открытый ключ (файлы .cer), который Вы можете передавать тем, кому сдаёте обменные файлы, и закрытый ключ (файлы .dat и пароль), который Вы никому не должны передавать, он нужен для подписи обменных файлов.

2. Устанавливаем «ПТ Користувач»

Это программа, которую распространяет ЦСК «Украинские специальные системы». С помощью неё можно подключать электронные ключи, проверять подпись, подписывать файлы и многие другие задачи с ключами. Если Вы приобрели электронную цифровую подпись у другого ЦСК, то программа и её установка могут быть другими.

Скачать установку «IIT Kopucmyвач»: <u>http://csk.uss.gov.ua/download/soft/Installs.rar</u>

Примечание: для установки необходимы права администратора.

Запустите файл EUInstall.exe. В зависимости от настроек операционной системы, может появиться окно «Предупреждение системы безопасности», тут надо нажать кнопку «Запустить».

В окне, что откроется, для продолжения нажмите кнопку «Далі».



Выберите пункт «Я приймаю цю угоду» и нажмите кнопку «Далі».

цензійна угода		6
Прочитайте цю важливу інформацію	о перед продовженням.	1
Прочитайте ліцензійну угоду. Ви по продовженням інсталяції.	винні погодитися з умовами цієї угоди пере,	д
Ліцензійна угода на програмний ко	омплекс користувача ЦСК "IIT Користувач	*
Програма являє собою комп'ютер носіях, та будь-яку "вбудовану" або	ну програму, записану на відловідних о електронну документацію.	III
Встановлюючи, копіюючи або інши самим приймаєте на себе умови ц угоди, негайно скасуйте інсталяція	м чином використовуючи програму, Ви тим џеї угоди. Якщо Ви не приймаєте умов цієї о програми.	
Програма захищена законами і мі право, а також іншими законами і	жнародними угодами про авторське договорами, що мають відношення до	Ŧ
Я приймаю цю угоду		

Выберите папку, куда следует установить программу, нажав кнопку «Змінити» или оставьте путь таким же. Нажмите кнопку «Далі».

IT Користувач ЦСК-1.3. Інсталяція	
Оберіть каталог для інсталяції програми	a constant
Куди необхідно інсталювати програму?	ľ
Програма буде інстальована у наступний каталог	19
Для продовження, натисніть Далі. Для вибору іншого ката Змінити.	алогу, натисніть
C:\Program Files\Certificate Authority-1.3\End User	Змінити
Необхідно мінімум 22,4 Мб дискового простору.	
Казад	Далі > Відміна

Нажмите кнопку «Далі».

Вкажіть ка	талог меню Пуск
Де потрібн	но розмістити значки швидкого запуску програми?
3	Значки швидкого запуску програми будуть записані у наступний каталог
Змінити.	овження, натисніть далі. Для виоору іншого каталогу, натисніть
ПТ\Корис	стувач ЦСК-1.3 Змінити

Укажите свой каталог для сертификатов, нажав кнопку *«Змінити»* или оставьте таким как задано. Это Вы зададите каталог для открытого ключа — он будет использоваться в следующем пункте. Нажмите кнопку *«Далі»*.

IIТ Користувач ЦСК-1.3. Інсталяція	
Вкажіть каталог для сертифікатів та СВС	2
Де створити каталог для сертифікатів та СВС?	r
Вкажіть каталог для сертифікатів та СВС, натисніть Далі. Дл каталогу, натисніть Змінити.	ля вибору іншого
C:∖My Certificates and CRLs 13	Змінити
< Hasan	lani > Відміна

Оставьте настройки, как на картинке и нажмите кнопку «Далі».

Оберіть додаткові задачі		2
Які додаткові задачі мають бути в	иконані?	T.
Оберіть додаткові задачі, що прог натисніть Далі.	рама інсталяції повинна виконат	ги, потім
Додаткові значки:		
📝 Створити значок на робочому	столі	
Інші завдання:		
🔲 Завантажити програму після і	інсталяції	
🔲 Інсталювати драйвери електр	онного ключа	
	(Hasan Dani)	Bigwina

Нажмите кнопку «Встановити» и дождитесь окончания установки.

отовність до інсталяції		SP.
Все готово до інсталяції ІІТ Користу	увач ЦСК-1.3.	ľ
Натисніть Встановити для продовж хочете переглянути або змінити де:	ення інсталяції або натисніть Назад, якщо які параметри.	ви
Каталог для запису: C:\Program Files\Certificate Author	prity-1.3\End User	*
Програмна група: IIT\Користувач ЦСК-1.3		
Додаткові задачі: Додаткові значки: Створити значок на робочому	у столі	
		-
	*	

3. Добавляем электронные цифровые ключи

Теперь нам необходимо правильно расположить наши ключи, которые мы получили от ЦСК при покупке электронной цифровой подписи.

Открытые личные ключи и сертификаты центра имеют расширение .cer. Вы их должны скопировать в папку для открытых ключей, которую мы указали в пункте 2. В нашем примере это папка:

C:\My Certificates and CRLs 13

Скачать сертификаты Центра «Украинские специальные системы» (если Вы у них приобретали ключи) можно отсюда:

http://csk.uss.gov.ua/ca-certificates

Личные открытые ключи Вы получаете от ЦСК любым доступным способом или можно даже скачать с их сайта, так как эти подписи должны быть доступны всем, кто собирается проверять Вашу электронную цифровую подпись. Найти их можно по ссылке:

http://csk.uss.gov.ua/certificates-search

Более детально узнать о том, как получить открытые и закрытые ключи, читайте документацию ЦСК, электронную цифровую подпись которой приобрели.

Закрытые ключи Вы получаете лично в виде файлов .dat на каком-то носителе информации (диск, флешка и т. д.). Эти файлы вместе с паролем выдаются один раз и персонально. Копии их в ЦСК нет, потому старайтесь их не терять и не распространять, ведь каждый, кто заполучит закрытые ключи и Ваш пароль, сможет подписать обменные файлы Вашим именем, а новую электронную цифровую подпись придётся получать заново!

Для закрытых ключей нужно определится, где мы их будем хранить. Это может быть как отдельное usb-устройство, диск, флешка, так и персональная папка на Вашем компьютере. В нашем примере мы рассмотрим вариант, когда закрытый ключ хранится в папке *C:\Sign*. Этот вариант подойдёт, если данным компьютером пользуетесь только Вы. В других случаях будет лучше хранить закрытые ключи на своей персональной флешке.

Запустите программу **KMFileSystemConfiguration.exe** (идёт вместе с установкой *«IIT Користувач»*). Нажмите кнопку *«Додати...»*

💫 IIT НКІ. Конфігурація файлової системи (каталогів)
ит Носії ключової інформації Конфігурація файлової систёми (каталогів)
Зареєстровані каталоги Каталоги
Не зареєстровано жодного каталогу

В окне *«Каталог з ключовими даними»* нажмите кнопку *«Встановити»* и в следующем окне выберите папку, куда скопировали свои закрытые ключи. Нажмите кнопку *«ОК»*.

	Розміщення каталогу
аталог з ключовими даними	Розміщення каталогу на файловій системі
Параметри каталогу з ключовими даними Назва каталогу:	▷ Scan ▷ Sign ▷ Temp ▷ wind2
Розміщення на файловій системі:	Vindows
Тип каталога (параметра): © системи © користувача	М Книги Книги Пользователи В ШАБЛОНИ В ШАБЛОНИ В ШАБЛОНИ В СТОР
	Создать папку ОК Отмена
🕦 Не зареєстровано жол	дного каталогу

Вернувшись в предыдущее окно, выберите «користувача» и нажмите кнопку «ОК».

Параметри каталогу з ключе	рвими даними	
Sign		
озміщення на файловій системі:		
C:\Sign		Встановити
Тип каталога (параметра): 🔘 системи	ОК	Відміна

Теперь у Вас сконфигурирована папка для закрытого ключа. Таким образом можно создавать несколько папок для разных подписей (если пользователей этого ПК несколько). Это окно можно закрывать.

ПТ НКІ. Конфігурація ПТ Носії к. Конфігурац	файлової системи (кат ПЮЧОВОЇ ІНФО ія файлової системи	алогів) ОМАЦІЇ (каталогів)	//
Зареєстров	ані каталоги	Каталоги Э Додати Э Змінити Видалити	
Інформація про к Назва каталогу: Sig Розміщення: С:	аталог: n Sign		

Чтобы проверить правильно ли Вы всё сделали, запустите программу «*ШТ Користувач ЦСК-1.3»* и перейдите в меню «*Особистий ключ»*.



Выберите команду «Зчитати...».

айли С	Собистий ключ Сертифікати та СВС Параметри Допомо	ora	
7 8	Зчитати	Ctrl+K	
×к	Переглянути власний сертифікат		
06	Згенерувати ключі		
00	Сформувати запит на сертифікат (зовнішній)		
	Резервне копіювання особистого ключа		
Jaco	Змінити пароль захисту особистого ключа		
9	Знищити особистий ключ на носієві ключової інформ	лації	
	Зтерти особистий ключ з пам'яті програми	F12	
	Перегляд сертифікатів у Перегляд СВС у файловому сховищі сховищі	файловому	
Додат	ково		
0	lерейти до web-сайту ЦСК		

Вы перейдёте в специальный режим защищённого рабочего стола, где надо выбрать свой метод расположения закрытого ключа. В нашем случае, надо выбрать *«файлова система (каталоги користувача)»*, откроется список заданных выше источников и выделить *«Sign»*. Это папка для нашего примера, где лежат закрытые ключи, у Вас она может быть другая.

Если же закрытые ключи Вы сохранили другим методом (например на флешке), то используйте соответствующий выбор источников.



В поле «Пароль» введите свой пароль для закрытого ключа и нажмите кнопку «Зчитати».

Если Вы сделали всё правильно и проверка ключей прошла успешно, то внизу отобразится фраза «Особистий ключ зчитано».



Если у Вас выдало какую-то ошибку, обращайтесь в соответствующий ЦСК, где приобретали подпись или прочитайте выше написанное ещё раз, чтобы проверить всё ли правильно Вы сделали.

4. Экспорт обменного файла XML из GIS 6 с электронной цифровой подписью

Вот мы и подошли к моменту работы с электронной цифровой подписью в GIS 6. Подразумевается, что Вы без проблем прошли все пункты 1-3. Если у Вас нет электронной цифровой подписи или на этапе проверки возникли проблемы, обращайтесь непосредственно в техподдержку ЦСК.

<u>Имейте ввиду: экспорт обменных файлов производится только при наличии технической</u> <u>поддержки у пользователя. Если она у Вас закончилась, необходимо её продлить, иначе</u> <u>обменные файлы создаваться не будут!</u>

Для начала настроим **GIS 6**, чтобы он автоматически подписывал обменные файлы, которые мы экспортируем. В главном окне *«Земельные участки»* перейдите в меню *«Сервис»* - *«Установки»*.

мационн	ная Система 6.1.7.6 Professional - [Земельные участки]						
Поиск	Отбор Расчёты План Агрогруппы Списки Печать Импорт Экспорт	Сервис Ок	:Ha ?				
1	, 📚 🎄 👔 🐘 Участок Харківська область, Лозівський район, Царедарівська біл	Установк	и				
er 80	 ۲ ۲ ۲ ۲ ۲ ۲ 	Запись б Дополне	аз данных на диск (архивиро ние из базы данных	вание)		- Uam	
номер	Адрес земельного участка	Присвои	ть всем отмеченным участка	им выбранные значения текущей запис	и		
04:0003	Участок № 001	Присвое	ние и замена значений полеі	ň			
04:0003	Участок № 002	Автонум	ерация отмеченных земельн	ых участков			
)4:0003	Участок № 001	Автонум	ерация отмеченных земельн	ых участков в разрезе КОАТУУ			
04:0003	Участок № 002	Автомат	ическое определение категор	ии земель			
	Київська область, Броварський район, смт Велика Димерка, пров. Леніна	Автомат	ическое созлание межевых з		TKOB		
06:0000	Київська область, Бородянський район, с. Небрат, вул. Кірова, 23	Abroman	пеское создание межерож з	lakes providence and the semicirclass y rac	ROD		
01:	Вишнівська сільська рада, Татарбунарський район, Одеська область (за межами насел	ел Автоматическое присвоение кадастрового номера Ctrl+			Ctrl+K	L	
00:0000	Одеська область, Кілійський район, с. Десантне, вул. Центральна, 5	Автомат	ическое определение квартал	па и присвоение кадастрового номера	Ctrl+S	Іокумент	
01:	Грушинська, буд. 30, м. Первомайський Харківської області	Расчёт де	енежной оценки земельного	участка	F11		
	Ділянка № 001	Созлании	е счетов в программе "Учёт d	инансового обеспечения"			
04:0001	с. Черкаські Тишки, вул. Арсентієва, 22-а	Проверка опраты в программе "Учёт финансового обеспечения"					
00:0702	Миколаївська область, Кривоозерський район, Секретарська сільська рада	проверк	а оплаты в программе эчег	финансового обеспечения			
01:	с. Крижанівка, вул. Бескоровайнова, 35 А	Создание счетов в программе "Электронный журнал регистрации клиентов"					
01:	с. Крижанівка, вул. Бескоровайнова, 35 А	Проверк	а оплаты в программе "Элек	тронный журнал регистрации клиенто	в"		
33:0001	Одеська область, м. Одеса, вул. Лінія 43, 30-а	Decreation			Ctrl E12		
07:0066	Київська область, Богуславський район, м. Богуслав, вул. 40 років Перемоги, 82		ма проверки лите файлов		CUITFIZ		
11:0027	Київська область, Броварський район, с. Погреби, вул. Горького		Параметры досупа к gistile.com				
01:	с. Крижанівка, вул. Бескоровайнова, 35 А	і ірава дл	ія групп пользователеи				
01:0615	с. Старі Боровичі, вул. Щорса, 101	Админис	трирование			цілянку	
00:0000	Одеська область, Фрунзівський район, смт Фрунзівка	Копия ба	зы данных				
	11Ц1.5034 Опора ЛЕП 10 кВ №124 Л-56 Василівська сільська рада, Солонянський райо	Подписа	ть файлы электронной подпи	ИСЬЮ			
00:1096	Волинська область, Луцький район, смт Рокині	0,0342					
	Житомирська область, Житомирський район, Зарічанська сільська рада с.Зарічани	1,8400	Книга регистрации				
00:0002	Одрадівська сільська рада, Первомайський район, Харківська область	7,9572	Номер/за номером	1			
01:0369	Житомирська область, Житомирський район, Зарічанська сільська рада с. Зарічани	0,0373	померлза номером	· · · · · · · · · · · · · · · · · · ·			
01:	Іржавецька сільська рада	10,1273		504			
01:1414	Іржавецька сільська рада	71,7121	Дата регистрации	02.01.2003			
01:	Іржавецька сільська рада	10,1273					
01:1414	Іржавецька сільська рада	71,7121					
	13B4.5017 КВК 580, охоронний стовп, охоронний кабельний стовпчик Дмитрівська сільс	0,0004					
0.0208	Харківська область. Позівський район. Царедарівська сільська рада, ділянка № 403	7 1056					

На закладке «Обменный файл XML» поставьте птичку «Электронная подпись».

👖 Установки системы	
Файл	
Реквизиты Отчётные формы Путь к служебным файлам Обменный файл Хм	I Обменный файл In4 Расчёты Рисунок МарDraw Прочее Смежества Денежная оценка Теодолитны
Формирование обменного файла кадастровой информации Xml	Региональные настройки
Формирование дополнительных тегов	Національна кадастрова система (НКС) 🔹
Перезаписать файлы с одинаковыми наименованиями	🥅 Адаптирование обменного файла под постановление 1051
Экспорт земельных участков в один обменный файл 🛛 🛛 🦎	🥅 Адаптирование обменного файла под приказ 323
Автоматическое заполнение данных	🔽 Электронная подпись
Дата по умолчанию 30.12.1899 💌 🥌	
Авто-заполнение улицы и номера дома 🛛 🦷	Формат наименования файла
Авто-проверка латинских символов 🛛 🔽	кадастровый номер (без разделителей) 🔹
Расчёт периметра без округлений 🛛 🔽	, Номер угодий (тег - CadastralCode)
Атоматическая проверка обменного файла 🛛 🗌	номер объекта 00:000
Формирование координат кадастрового квартала (тег CadastralQuarters) 🔽	Формат заполнения аренды/субаренды
Формировать в блоке "Смежники" направляющие стрелок 🔽 🔽	только Leases
Очищать тег PN для стрелок смежества 🔽 🔽	Формат заполнения сервититов
Проверять формат заполнения смежников через запятую 🔽	
Формирование адреса с сокращениями 🔽	
Автоматическое формирование блока угодий 🛛 🔽 🔽	Код документа (тег - Document)
Код угодий по форме 6 зем (по умолчанию) 05	код из классификатора Xml (приложение № 23) 🔹
Формировать несколько решений у одного субъекта права 🛛 🗌	Имя узла полигона (тег · PN)
Заполнение кода КВЦНЗ с буквой секции (А.01.01)	С номер точки С по порядку 💽 имя точки
Объединять договора аренды, если совпадает арендатор (тег - Leases) 🛛 🔲	Вид документа в аренде (тег ApprovalDocument)
Формирование срока договоров аренды (тег - LeaseDuration) 🛛 🗌	С дополнение 37 . С дополнение 23
Формирование пустых дескрипторов 🔽 🔽	Дополнительная информация о субъектах (теr AdditionalInfo)
Полилинии в виде отрезков 🔽 🔽	 наименование док комментарии суртавто-заполнение
Метрическая информация без параметров Н и МН	Формат сохранения государственного акта (rer StateActInfo) Савто-выбор последнего С сохранение всех
Заполнение тега PointInfoDescription 📃	Формат заполнения государственного акта

Сохраните настройки нажав кнопку «Сохранить».

После этой небольшой настройки, все файлы XML, которые Вы будете экспортировать, будут также автоматически подписываться. После экспорта появится диалоговое окно «Зчитування особистого ключа», где надо выбрать тот вариант хранения ключа, которым Вы пользуетесь. В нашем примере это отдельная папка на диске, потому выделяем «Файлова система (каталоги користувача)».

a second second	-1.2 ···	формація про носіи.
оптичний диск е ключ IIT Кристал-1 е ключ IIT Кристал-1 (носій) файлова система (каталоги системи) файлова система (каталоги користувача) © Sign смарт-карта Техноконс. TEllipse смарт-карта Техноконс. TEllipse2/3	Тип:	файлова система (каталоги користувача

Появятся папки, которые мы зарегистрировали с помощью программы **KMFileSystemConfiguration.ex**е. Выбираем эту папку, вводим пароль для закрытого ключа и нажимаем «*OK*».

🐙 гнучкий диск	🔫 Інформація про носій:
и з сипии диск е ключ IIT Кристал-1 е ключ IIT Кристал-1 (носій) файлова система (каталоги системи) файлова система (каталоги користувача) © Sign Смарт-карта Техноконс. TEllipse смарт-карта Техноконс. TEllipse2/3	Тип: файлова система (каталоги користувача) Назва: Sign

В результате на диске появятся два новых файла .xml и .p7s. Первый — это обычный обменный файл не подписанный, а второй — это подписанный файл XML. Если хотите передать подписанный файл, то передавайте только файл .p7s !

5. Проверка электронной цифровой подписи и импорт подписанного обменного файла XML в GIS 6

Если Вы хотите только проверить электронную цифровую подпись, то используйте для этого программу *«ШТ Користувач»*. Если же хотите импортировать **XML** в **GIS 6**, то делайте это обычным образом, как импортируются все остальные обменные файлы, только выбирать надо файл **P7S**. Программа сразу проверит электронную цифровую подпись. Если проверка прошла удачно, файл будет импортироваться в **GIS 6**. Если файл был изменён не владельцем или электронная цифровая подпись была не правильна, **GIS 6** выдаст ошибку.

овідомл	ення оператору
×	Виникла помилка при перевірці підпису файла Опис помилки: Невірний підпис
	ОК

Такой обменный файл Вам не удастся импортировать.

Если у Вас не установлена программа *«IIT Користувач»* и/или не добавлены сертификаты открытых ключей пользователей, обменник, который импортируете, то, при проверке электронной цифровой подписи, программа может выдать сообщение, что сертификат не определён.

Сертифікат м не визначен	южливо н ий. Викори	е чинний або йог истати його?	о статус
Осертифікат		Так	Hi
Результати пошуку та в	изначення с	татусу:	
Перевірка сертифіката сховищі	Перевірка сертифіката у файловому сховищі		анцюжку не
Пошук чи перевірка сертифіката через OCSP-сервер		Не виконувався	
Інформація про сертифі	кат:		
🔄 Власник	test		
🔄 ЦСК	АЦСК ДП "	VCC"	
РН сертифіката відкр.	425D4BC6E	44FFB100400000010000	002A000000

Если хотите продолжить и всё таки импортировать файл, нажмите кнопку «Так».