

## ИНФОРМАЦИОННЫЙ ЛИСТ

### Услуги Центра сертификации ключей «MASTERKEY»



## Услуги Центра сертификации ключей «MASTERKEY»

Для осуществления деятельности в области электронной цифровой подписи (ЭЦП) Центры сертификации ключей (ЦСК) компании «Арт-мастер» предоставляют следующие услуги:

1. Регистрация клиентов.
2. Генерация ключей ЭЦП, формирование Сертификатов открытых ключей.
3. Предоставление программного обеспечения для использования ЭЦП и для криптографической защиты электронных документов.
4. Предоставление услуги блокирования, восстановления и аннулирования Сертификатов открытых ключей клиентов ЦСК.
5. Публикация списков заблокированных и аннулированных Сертификатов открытых ключей клиентов на web-сайте ЦСК.
6. Предоставление услуги формирования отметки точного времени.
7. Подтверждение подлинности ЭЦП электронных документов.

Услуга № 7 предоставляется только Аккредитованным центром сертификации ключей «MASTERKEY».

В этом информационном листе раскрывается суть и назначение предоставляемых ЦСК услуг. Общий порядок предоставления услуг ЦСК описывается в информационном листе «Как стать клиентом Центра сертификации ключей «MASTERKEY»».

### **1. Регистрация клиентов.**

Регистрация клиента проводится в офисе ЦСК. Процедура регистрации включает в себя процесс идентификации клиента и заключение договора на предоставление услуг ЭЦП (далее Договор).

Идентификация клиента позволяет установить связь между юридическим или физическим лицом и конкретной ЭЦП. Законодательство в области ЭЦП возлагает на ЦСК обязанность установить такую взаимосвязь.

Идентификация осуществляется на основании документов, позволяющих однозначно определить лицо, обратившееся в ЦСК.

Копии представленных для идентификации документов составляют основу личного дела клиента. Полученная таким образом информация используется при подготовке всех необходимых для предоставления услуг ЭЦП документов и заключения Договора.

После процесса регистрации личное дело клиента попадает в специализированное хранилище, которое обеспечивает гарантированную защиту персональных данных.

Полученные данные хранятся на протяжении всего срока функционирования ЦСК. В случае прекращения деятельности ЦСК документы не уничтожаются, а передаются для дальнейшего хранения в Центральный удостоверяющий орган.

### **2. Генерация ключей ЭЦП, формирование Сертификатов открытых ключей.**

Генерация ключей ЭЦП происходит в кабине генерации ключей при помощи специального программно-аппаратного комплекса,

эффективность защиты которого подтверждена соответствующим экспертным заключением.

Процедура генерации ключей ЭЦП позволяет клиенту получить:

- личный ключ ЭЦП;
- открытый ключ ЭЦП, который содержится в соответствующем разделе Сертификата открытого ключа.

Личный ключ ЭЦП формируется на основании случайных чисел, получаемых с помощью генератора случайных чисел.

Генератор случайных чисел может быть:

- программным (принцип действия базируется на основе программных алгоритмов);
- аппаратным (принцип действия основан на регистрации физических процессов - внутренних шумов устройств).

В ЦСК компании «Арт-мастер» применяется аппаратный способ генерации случайных чисел. Он полностью исключает возможность повторения чисел с течением времени.

Личный ключ ЭЦП нужен клиенту для подписания электронных документов. Данные личного ключа ЭЦП - секретная информация, которую должен знать исключительно владелец личного ключа.

Открытый ключ ЭЦП вычисляется из личного ключа таким образом, чтобы получить личный ключ из открытого было невозможно. Открытый ключ ЭЦП однозначно соответствует личному ключу.

На основании информации, полученной при регистрации клиента, и данных открытого ключа формируется Сертификат открытого ключа.

Сертификат открытого ключа позволяет определить срок действия пары ключей и принадлежность открытого ключа тому, кто подписал электронный документ.

В Сертификате открытого ключа обязательно содержится следующая информация:

- наименование и реквизиты ЦСК;
- указание на то, что Сертификат открытого ключа выдан в Украине;
- уникальный регистрационный номер Сертификата открытого ключа;
- основные данные (реквизиты) владельца личного ключа;
- дата и время начала и окончания срока действия Сертификата открытого ключа;
- открытый ключ;
- наименование криптографического алгоритма, который используется владельцем личного ключа;
- информация об ограничениях использования ЭЦП.

Кроме обязательной информации, в Сертификате открытого ключа по усмотрению клиента могут указываться дополнительные данные.

Целостность и неизменность информации, указанной в Сертификате открытого ключа клиента, подтверждается путем наложения на него ЭЦП ЦСК.

### **3. Предоставление программного обеспечения для использования ЭЦП и для криптографической защиты электронных документов.**

Функционирование ЭЦП поддерживает специализированное программное обеспечение «Программный комплекс користувача ЦСК», в котором реализовано 4 основные функции:

- подписание документа;
- проверка подлинности ЭЦП на полученных документах;
- шифрование документа;
- дешифрование документа.

Программное обеспечение удобно в использовании и не требует специальных навыков по его использованию. «Программный комплекс користувача ЦСК» можно загрузить с web-сайтов Центров сертификации ключей [www.masterkey.com.ua](http://www.masterkey.com.ua) или [www.cskkey.kiev.ua](http://www.cskkey.kiev.ua).

### **4. Блокирование, восстановление и аннулирование Сертификатов открытых ключей клиентов ЦСК.**

Сертификату открытого ключа может быть присвоен один из трех статусов: действующий, заблокированный, аннулированный.

Статус «действующий» присваивается Сертификату открытого ключа автоматически при его формировании. Срок действия Сертификата определяется условиями Договора, но не может превышать 24 месяца с момента формирования. Статус Сертификата открытого ключа «действующий» означает, что подписание документа легитимно и имеет юридическую силу.

Статус «блокированный» присваивается Сертификату открытого ключа:

- если клиенту необходимо приостановить (путем личного обращения в офис ЦСК) использование ЭЦП на определенный срок, превышающий 10 дней. По истечении этого срока статус «действующий» Сертификату открытого ключа присваивается автоматически;
- если Сертификат открытого ключа был заблокирован (путем телефонного обращения) без указания срока восстановления. По истечении семи дней с момента блокирования его статус переходит в «аннулированный»;
- в случае подозрения на компрометацию<sup>1</sup> личного ключа, до момента выяснения обстоятельств. Если блокирование Сертификата открытого ключа осуществлялась по телефону, срок выяснения обстоятельств не должен превышать семи дней. В противном случае Сертификату открытого ключа будет автоматически присвоен статус «аннулированный».

Статус «аннулированный» присваивается Сертификату открытого ключа:

- обязательно в случае компрометации личного ключа клиента, причем о факте компрометации клиент должен уведомить ЦСК;
- если клиент принял решение о прекращении использования ЭЦП;
- если Сертификат открытого ключа был заблокирован без указания срока восстановления (путем телефонного обращения), по истечению семи дней с момента блокирования.

Аннулированный Сертификат открытого ключа восстановлению не подлежит. В этом случае для возобновления использования услуги ЭЦП необходимо провести процедуру генерации ключей ЭЦП заново.

### **5. Публикация списков заблокированных и аннулированных Сертификатов открытых ключей клиентов на web-сайте ЦСК.**

Информация о статусе Сертификата открытого ключа позволяет определить легитимность ЭЦП полученных электронных документов.

<sup>1</sup>Компрометация личного ключа ЭЦП - его потеря или использование посторонними лицами, повреждение носителя ключевой информации. Использование скомпрометированного ключа запрещено.

Статус «действительный» свидетельствует о том, что электронные документы подписаны легитимной ЭЦП. Статусы «блокированный» и «аннулированный» свидетельствуют о том, что доверять ЭЦП полученных электронных документов нельзя.

Для того чтобы участники электронного документооборота могли отслеживать статус Сертификата открытого ключа подписанных электронных документов, на web-сайте ЦСК публикуются списки заблокированных и аннулированных Сертификатов открытых ключей клиентов.

Специализированное программное обеспечение «Программный комплекс користувача ЦСК» может быть настроено таким образом, чтобы при проверке ЭЦП поступивших электронных документов автоматически проверялся статус используемых при их подписании ключей.

### **6. Предоставление услуги формирования отметки точного времени.**

При утверждении электронных документов с помощью ЭЦП важно знать дату и время наложения ЭЦП. ЦСК предоставляют услугу по формированию отметки точного времени при подписании электронных документов.

Отметка точного времени позволяет с точностью до одной секунды определить время наложения ЭЦП, причем изменить отметку точного времени невозможно. Возможно лишь повторное подписание электронного документа с фиксацией нового времени.

Процесс получения отметки точного времени выполняется автоматически при выборе клиентом соответствующих настроек программного обеспечения.

Оборудование ЦСК, формирующее отметку точного времени, синхронизировано с Всемирным координированным временем (UTC) и получает информацию о точном времени через спутниковые каналы связи.

### **7. Подтверждение подлинности ЭЦП электронных документов.**

В процессе электронных отношений у клиента могут возникать спорные вопросы относительно подлинности ЭЦП в электронных документах.

Для решения этих вопросов ЦСК «MASTERKEY» предоставляет услугу удостоверения подлинности ЭЦП в электронных документах.

Результатом предоставленной услуги является письменное заключение ЦСК «MASTERKEY», которое может быть представлено в качестве доказательства в судах или других инстанциях.

Более подробную информацию об этом можно узнать из информационного листа «Подтверждение подлинности Электронной цифровой подписи электронных документов».

Услуги ЭЦП предоставляют два ЦСК, которые являются структурными подразделениями компании «Арт-мастер»:

- неаккредитованный центр сертификации ключей;
- аккредитованный центр сертификации ключей «MASTERKEY».

Более подробная информация о ЦСК изложена в информационном листе "О центрах сертификации ключей ООО «Арт-мастер».

Деятельность компании в области предоставления услуг ЭЦП была сертифицирована в 2006 году согласно требованиям международного стандарта менеджмента качества ISO 9001:2000.

Подробную информацию о том, что такое центры сертификации ключей вы можете найти, обратившись к информационному листу «О центрах сертификации ключей компании «Арт-мастер».

Подробную информацию о том, что такое ЭЦП и как она функционирует, можно узнать из информационного листа «Электронная цифровая подпись и ее функционирование».



ООО «Арт-мастер»  
ул. Сурикова, 3 (лит. А), Киев, 03035, Украина  
тел.: +380 44 248-97-91, 248-98-27, 248-98-28, факс: +380 44 248-98-14  
e-mail: post@am-soft.com.ua; http://www.am-soft.com.ua



Центр сертификации ключей «MASTERKEY»  
ул. Сурикова, 3 (лит. А), 4 этаж, Киев, 03035, Украина  
тел.: +380 44 206-13-78, тел./факс: +380 44 206-13-79  
info@masterkey.com.ua www.masterkey.com.ua