

Сравнительный анализ технологий, выполняющих процедуру заверения электронного документа

Действие	Выработка дополнительной ЭЦП	Специализированный сервис DVCS
Форма ответа	Добавление ЭЦП в исходный документ. Порождается перечень сопутствующих задач, требующих формализации и решения в рамках конкретной ИС: формализация процедуры проведения последующих проверок, очередность их выполнения, факты авторства документа, протокол проведения проверки и т.п.	Определена в международных рекомендациях на DVCS
Место выполнения процедуры заверения электронного документа	1. На рабочем месте уполномоченного лица. Порождает проблемы обеспечения безопасности и сохранения в тайне закрытого ключа. 2. На выделенном сервере. Порождает проблемы создания протокола взаимодействия рабочих мест с сервером, отражающего также алгоритм такого взаимодействия	В специализированном сервере по протоколу DVCS. Легко обеспечить условия безопасности и сохранность в секрете закрытого ключа (или ключей в режиме депонирования) уполномоченного лица
Возможность проведения неправомерных действий уполномоченного лица	Присутствует. В алгоритме оказания услуги отсутствует документальное оформление доказуемого этапа проведения предварительных проверок принятого электронного документа. Другими словами, уполномоченное лицо может выработать свою ЭЦП, не проводя исходных проверок. Данное действие, конечно, будет раскрыто во время проведения разбора ситуации, но технически такого рода "заверенный" документ может быть внедрен в систему ЭДО, что может повлечь за собой значимые последствия еще до начала организации разбора конфликта	Принципиально исключает такую возможность, так как квитанция содержит заверенные результаты проверок исходных подписей и политик и криптографически связана с исходным документом и ЭЦП. Подложная квитанция будет отбракована уже при первой попытке ее использования. DVCS исключает человеческий фактор и не позволяет использовать недействительные документы, не ожидая этапа разбора конфликта
Проверка на правомочность ЭЦП на исходных электронных документах	В явном виде отсутствует и требует разработки специализированного ПО и формализации регламента выполнения таких процедур	Штатная функция протокола – проверка ЭЦП на соответствие политики использования сертификата, через которую и указывается правомочность автора ЭЦП
Компрометация закрытого ключа на рабочем месте уполномоченного лица	Приводит к компрометации всей системы. Минимизировать последствия можно в случае делегирования функции заверения специализированному серверу, но в этом случае потребуются разработка протокола и регламента взаимодействия рабочих станций и сервера	На безопасность не влияет, процедуры проверок и заверения выполняются на стороне сервера по протоколу, определенному международными рекомендациями
Длительное архивное хранение заверенного электронного документа с сохранением юридически значимых последствий	Для пролонгации ЭЦП уполномоченного лица заверяющего документа требуется извлекать исходный документ из архива. При больших объемах хранилища данная проблема усугубляется еще и необходимостью транспортировки больших объемов данных по компьютерным сетям с обеспечением их конфиденциальности. Для выполнения всех этих процедур следует разработать специальное ПО и формализовать их алгоритмически	При пролонгации заверяется предыдущая квитанция очень маленького размера, исходный документ из архива не извлекается. Данная процедура предусмотрена протоколом, и она выполняется автоматически внутри самого DVCS-сервера. В данной процедуре прикладная система (архив) не участвует
Юридическое значение действия заверения	Личная ответственность уполномоченного лица как владельца закрытого ключа в соответствии с ФЗ "Об ЭЦП" и в объеме своих штатных или профессиональных обязанностей	Два различных режима. 1. Личная ответственность уполномоченного лица как владельца закрытого ключа в соответствии с ФЗ "Об ЭЦП" в объеме своих штатных или профессиональных обязанностей для уровня корпорации, организации или национально-отраслевой структуры. 2. Личная ответственность уполномоченного лица как владельца закрытого ключа в соответствии с ФЗ "Об ЭЦП" через авторизованное использование депонированного в HSM-сервер закрытого ключа, на котором формируется ЭЦП на квитанции, и в объеме своих штатных или профессиональных обязанностей