Таблица 2. Сравнение некоторых характеристик PKI-сервисов на основе ETSI TS 101 733 (улучшенная ЭЦП) и RFC 3029

Характеристика	ETSI TS 101 733 (УЭЦП)	RFC 3029 (DVCS)	Вывод
Архитектура	Клиентское решение (формирование и проверка УЭЦП происходит на стороне клиента). **Е.П.:** Также считаем, что это не является услугой	Клиент-серверное решение. Сервер позиционируется как доверенная третья сторона (ДТС), или Trusted Third Party (TTP). Технологически услуга может быть оформлена как SaaS (Software as a Service – ПО как услуга). **Е.П.:** Это является услугой	Рассматриваемые технологии имеют различную архитектурную основу
Назначение	Расширенная спецификация ЭЦП, дополнительно включающая: механизм доказательства момента подписи документа и действительности сертификата ключа подписи на этот момент; механизм подтверждения действительности сертификата автора ЭЦП с отсутствием необходимости сетевых обращений при условии, что политика безопасности предполагает безусловное доверие к TSP- и OCSP-серверам. **Е.П.:** Согласны, это только формат подписи	Технология, позволяющая реализовать: подтверждение обладания информацией с/без ее предоставления сервису; проверку действительности ЭЦП на электронном документе; проверку действительности сертификата(ов) открытого ключа. **Е.П.:** Две функциональности в одной услуге – формат квитанции и протокол	Рассматриваемые технологии имеют различное назначение и предполагаются к применению в различных условиях с точки зрения требований по безопасности (в условиях различных моделей нарушителей)
Трансграничность применения	Обеспечивает посредством установки двух (или нескольких) независимых одна от другой ЭЦП на основе криптографических алгоритмов, принятых в государствах-участниках. В некоторых условиях (например, ограничение экспорта криптографических средств) осуществляется только одной ЭЦП, которая соответствует стандартам проверяющей стороны. ЭЦП противоположной стороны не проверяется. Решение о (не)возможности проверки ЭЦП противоположной стороны опирается на организационные мероприятия. **Е.П.:** Имеем много подписей, которые требуют проверки. Проверяющий может это сделать на основании клиентского программного обеспечения или пользуясь услугой. **А. С.-М.:** Кроме правовых аспектов использования соответствующих криптографических средств, описанных выше, возникает проблема изменений клиентского ПО с дистрибуцией самих криптосредств конечному пользователю, в связи с чем возникнут дополнительные расходы на информационный центр поддержки ПО клиента	Обеспечивается протоколами взаимодействия между TTP различных государств. Подтверждение ЭЦП противоположной стороны для конечного пользователя осуществляет TTP, действующий в рамках правового поля страны пребывания конечного пользователя. **Е.П.:** В этом помогает DVCS!!! **А. С.-М.:** При использовании различных криптографических систем в соответствующих странах является решением, которое в реальном времени можно настроить в серверной части на взаимодействие с соответствующей услугой проверки ЭЦП. При этом не происходят изменения в клиентской части, используемой конечными пользователями	Характеристики решений с точки зрения трансграничного применения ЭЦП различны. Для выработки решения о возможности применения каждого из решений в системах трансграничного электронного документооборота (ЭДО) требуется разработка модели угроз конкретных систем ЭДО, а также анализ правовых особенностей и технических решений у контрагентов
Документируемость факта проверки ЭЦП в электронном документе и времени проведения этой проверки	Основывается на требовании к ответственности пользователя, осуществляющего проверку; может быть дополнительно обеспечена организационными мероприятиями. **Е.П.:** После проверки подписи ETSI можно отметить ее временем (если раньше не была отмечена), как и все собранные во время проверки квитанции (сертификаты цепочки, CRL, OCSP). Однако нет доказательства того, что процесс проверки закончился (разве что в реестре событий). DVCS является в этом случае лучшим решением, поэтому он должен быть использован при проверке. **А. С.-М.:** К квитанциям при проверке подписи ETSI необходимо присоединить квитанцию DVCS с результатами проверки на определенный момент времени. Эта квитанция зафиксирует состояние проверки подписи документа, в противном случае необходимо будет его снова проверять при использовании и обращении к нему	Заверенный TTP электронный документ или квитанция содержит результат проверки и штамп времени. **Е.П.:** По моему мнению, это самый сильный аргумент решения DVCS. Не исключает он, конечно, использование формата ETSI (ведь это есть расширенный CMS, до проверки которого настроен также DVCS)	Для выработки решения о возможности применения каждого из решений в системах ЭДО требуется разработка модели угроз конкретных систем документооборота, а также анализ правовых особенностей и технических решений у контрагентов