Разъяснение по переходу на ГОСТ Р 34.10-2012

В соответствии с выпиской из документа ФСБ России от 31 января 2014 г. №149/7/1/3-58 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования», использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается, в том числе и для целей формирования списка отзыва сертификатов. После 31 декабря 2018 года формирование электронной подписи должно производится по алгоритму ГОСТ Р 34.10-2012.

Выпуск подчиненных сертификатов для аккредитованных удостоверяющих центров (далее – АУЦ) с использованием схемы подписи, установленной ГОСТ Р 34.10-2012, планируется начать в первом квартале 2018 года (соответствующее уведомление будет размещено на портале Федерального ситуационного центра электронного правительства).

Необходимо обратить внимание на то, что квалифицированные сертификаты со схемой подписи, отличной от схемы подписи сертификата АУЦ, выдавшего такой квалифицированный сертификат, на Едином портале государственных и муниципальных услуг (функций) (https://www.gosuslugi.ru/pgu/eds/) не будут проходить проверку.

Сценарии перевода пользователей на работу с квалифицированными сертификатами ключей проверки электронной подписи, выпущенные с использованием схемы подписи, установленной ГОСТ Р 34.10-2012, каждый АУЦ вправе выбрать по своему усмотрению исходя из особенностей регламента работы АУЦ, используемой информационной системы и других технических и организационных возможностей. В качестве примера может быть рассмотрен выпуск пользовательских сертификатов с использованием схемы подписи ГОСТ Р 34.10-2012 сразу после издания сертификата подчиненного АУЦ по ГОСТ Р 34.10-2012 и последовательный перевыпуск пользовательских сертификатов, выпущенных по ГОСТ Р 34.10-2001, до 31.12.2018.