О порядке перехода к использованию
новых стандартов ЭЦП и функции хэширования
№ 149/7/1/3-58 от 31.01.2014 **(выписка)**

Порядок перехода к использованию национального стандарта ГОСТ Р 34.10-2012 в средствах электронной подписи для информации, не содержащей сведений, составляющих государственную тайну, в случаях, подлежащих регулированию со стороны ФСБ России в соответствии с действующей нормативной правовой базой

Для средств ЭП, техническое задание на разработку которых утверждено после 31 декабря 2012 года, должна быть предусмотрена реализация функций средства в соответствии с ГОСТ Р 34.10-2012 хотя бы по одному из определяемых стандартом вариантов требований к параметрам (использование варианта, соответствующего длине секретного ключа порядка 256 бит, является предпочтительным, поскольку обеспечивает достаточный уровень криптографической стойкости и лучшие эксплуатационные характеристики, в том числе при совместной реализации со схемой ГОСТ Р 34.10-2001). После 31 декабря 2013 года не осуществлять подтверждение соответствия средств ЭП Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27.12.2011 г. № 796, если в этих средствах не предусмотрена реализация функций средства в соответствии с ГОСТ Р 34.10-2012 хотя бы по одному из определяемых стандартом вариантов требований к параметрам. Исключение может быть сделано для средств ЭП, удовлетворяющих одновременно следующим условиям:

- техническое задание на разработку средства утверждено до 31 декабря 2012 года;
- в соответствии с техническим заданием разработка средства завершена после 31 декабря 2011 года;
- подтверждение соответствия средства указанным Требованиям ранее не осуществлялось.

Использование схемы подписи ГОСТ Р 34.10-2001 для формирования подписи после 31 декабря 2018 года не допускается.