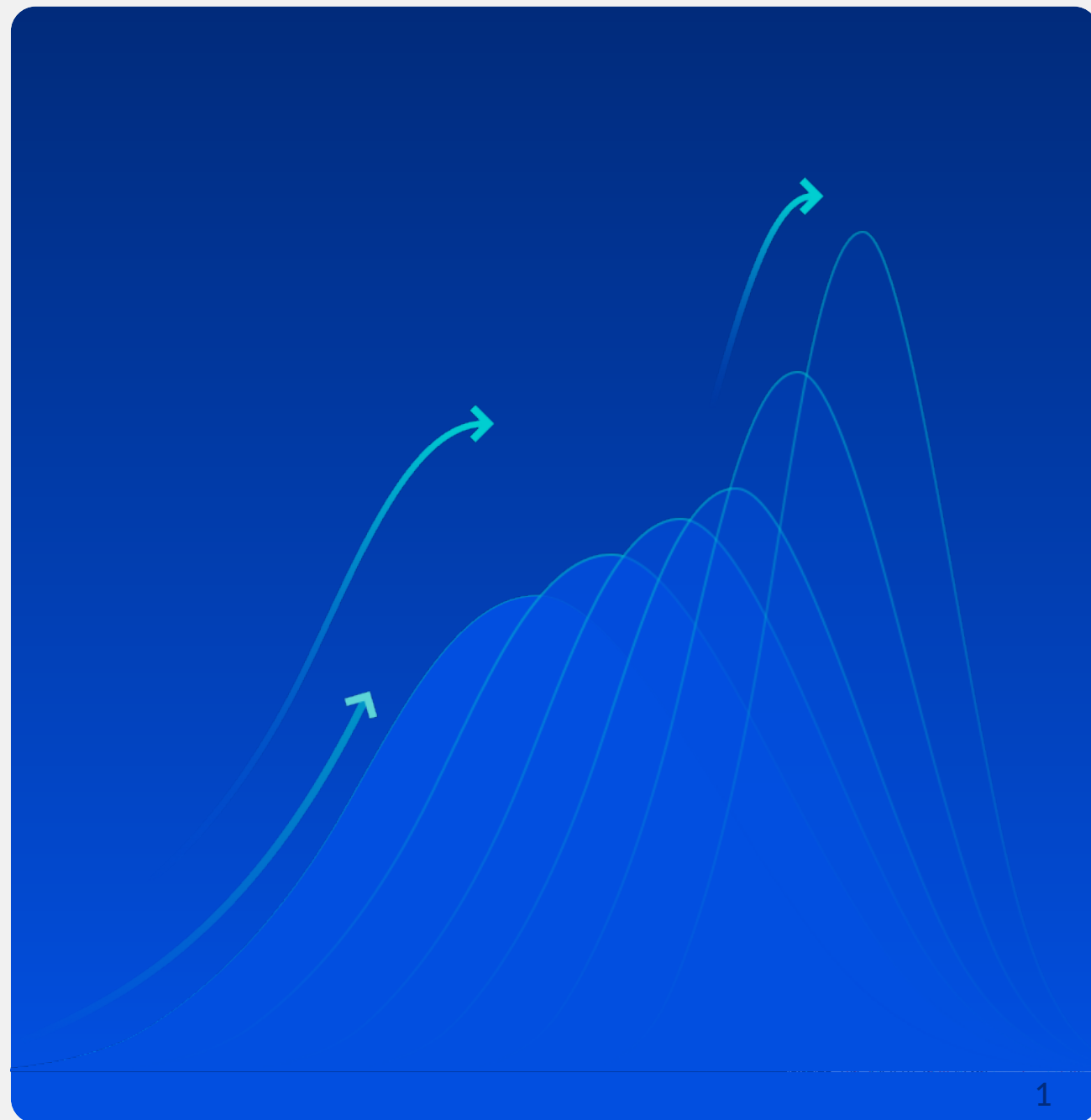


Реализация ДСЧ в СКЗИ для массового пользователя

CTCrypt 2025

Лебедев А. Н.

Вылегжанин Н. А.



Проблемы в продуктах с отечественной криптографией

В массовых СКЗИ существует проблема генерации «хорошей» случайности силами самих «простых» пользователей.

Есть либо АМДЗ, либо БДСЧ, что на пользовательских устройствах и в пользовательских сценариях - плохо.

В импортных средствах криптографической защиты такой проблемы нет в связи с использованием качественных встроенных аппаратных генераторов случайных чисел.

Проблемы в продуктах с отечественной криптографией

Обычная «Клавдия Ивановна» не понимает и потому воспринимает с недоверием процесс многократной генерации «чего-то случайного» путем «игры в рулетку» или нажатия случайных клавиш.

Процесс биометрической генерации случайной гаммы на мобильных устройствах не выглядит изящным.

В каждом сеансе ее генерации получается мало случайной гаммы.



Наше предложение

Скомбинировать
генерацию качественной гаммы только на сервере
и передачу ее в зашифрованном виде пользователям
для применения в качестве исходного материала
ключей ЭП,
ключей аутентификации,
рабочих ключей шифрования данных.

Наше предложение

Случайная гамма генерируется только на серверах сети с помощью сертифицированных отечественных аппаратных генераторов и проходит все необходимые тесты, прежде, чем высылается пользователям в зашифрованном виде (TLS, DTLS).

Ключи для ее шифрования вырабатываются по протоколу ECDHE с однократным использованием БДСЧ на стороне клиента.

Наше предложение

Следующие порции гаммы при отсутствии TLS, DTLS могут шифроваться на последнем отрезке предыдущей ее порции, который является общим секретным ключом сервера и пользователя для шифрования и передачи следующей порции случайной гаммы.

Авторы будут благодарны участникам
за конструктивную критику

**Спасибо
за внимание**

АО «Инфотекс Интернет Траст»

8 800 250-8-265

iitrust.ru