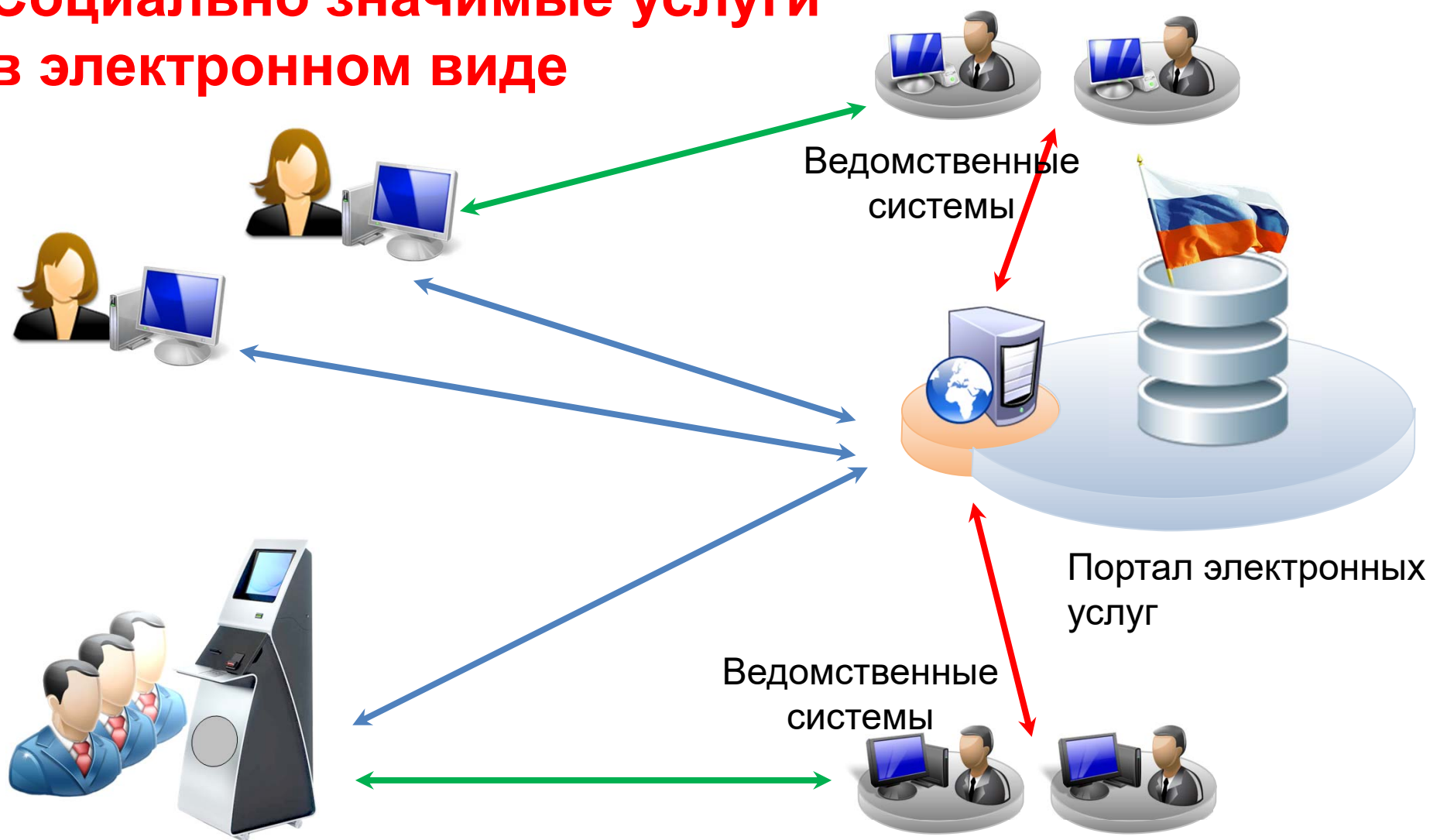


Некоторые аспекты использования криптографических средств при предоставлении государственных электронных услуг

Дмитрий Гусев
ОАО «ИнфоТеКС»
gusev@infotecs.ru

Социально значимые услуги в электронном виде



Особенности в предоставлении e-услуг



адресное предоставление услуг –
идентификация и аутентификация



юридическая значимость –
электронная подпись



удаленное взаимодействие
по сетям общего пользования –
защита каналов

средства
криптографической
защиты
информации



средства
защиты от НСД

Основные факторы



миллионы
абонентов



различная
квалификация



разнородные
информационные системы



территориальная
распределенность

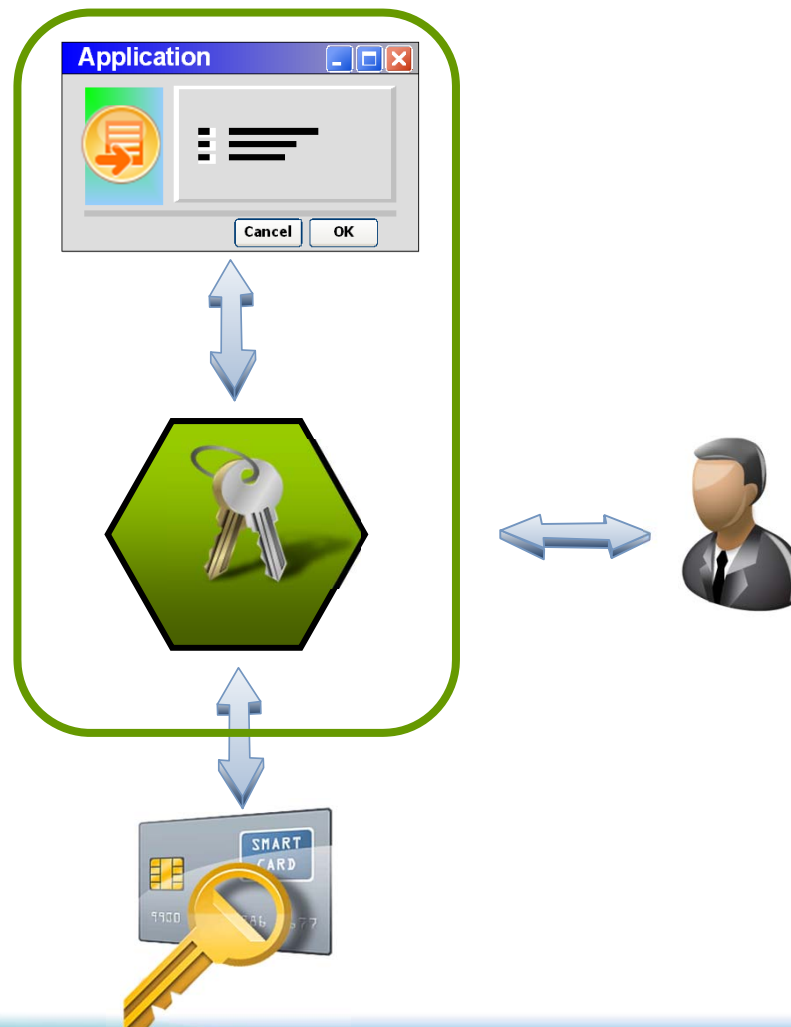
универсальное
решение
?

СКЗИ в компьютерной системе

функции защиты отделены от
прикладного функционала

криптопровайдер –
программный провайдер
криптографических функций

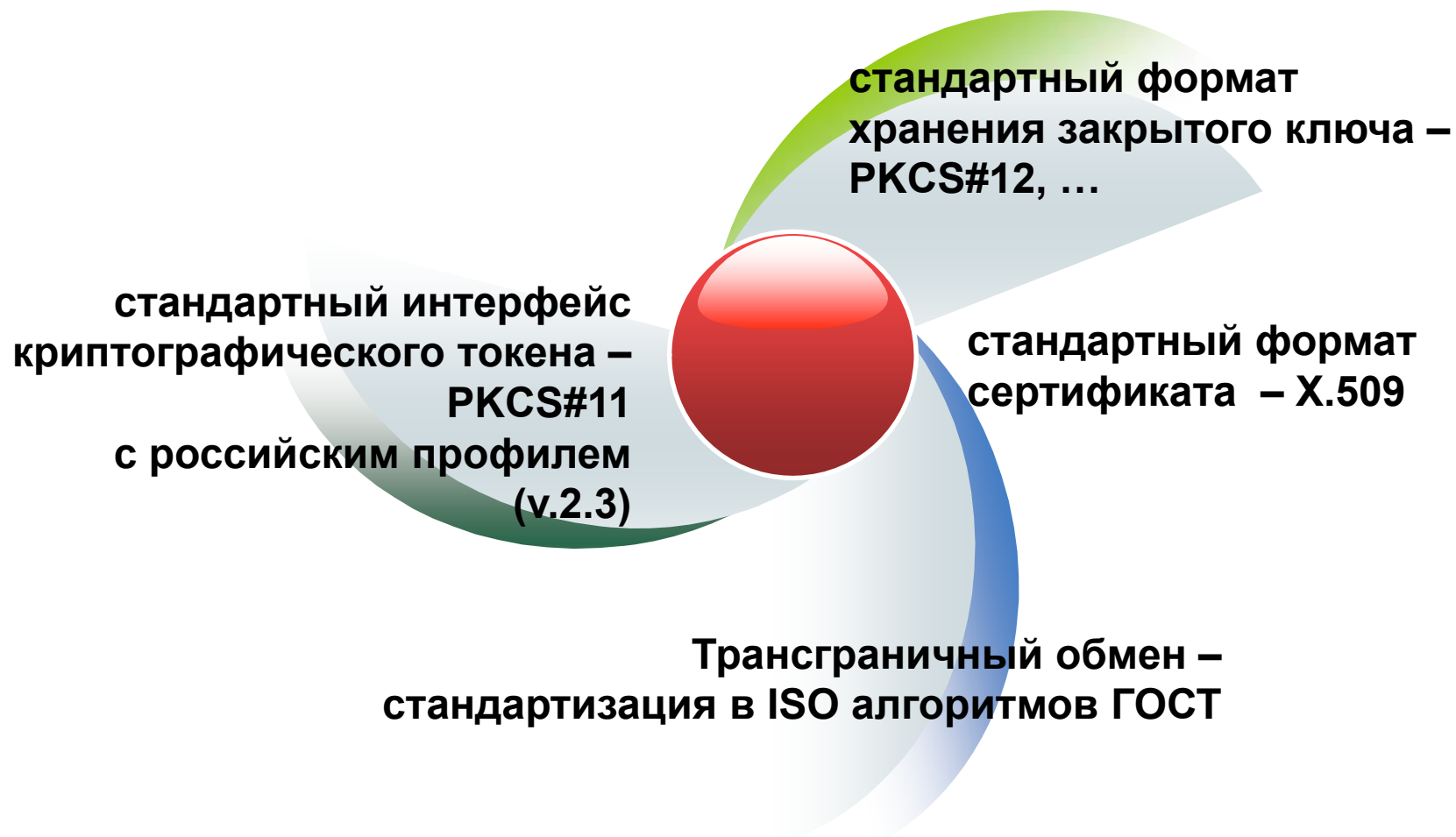
внешние ключевые носители
и аппаратные криптомодули



Совместимость российских СКЗИ

- ❑ Совместимость алгоритмов и форматов сертификатов ЭЦП – «соглашение пяти компаний»
- ❑ Совместимость форматов документов и транспортных протоколов – вопросы разработчиков систем документооборота
- ❑ Совместимость форматов хранения закрытых (секретных) ключей подписи – ?
- ❑ Совместимость электронных ключей (токенов) – ?

Путь к универсальным решениям



Инициативы компании ИнфоТеКС

- Продолжение активной поддержки «соглашения пяти...»
- Секретарская компания ТК26
- Ведение процесса стандартизации ГОСТ Р34.10-2001 в ISO
- Активное участие в разработке российского профиля PKCS#11 v.2.3
- Работа с производителями токенов по обеспечению совместимости на базе PKCS#11
- Совместное с компанией Сигнал-КОМ предложение по безвозмездной передаче своих CSP госорганам для предоставления е-услуг физ.лицам

Спасибо за внимание!

Вопросы?

Дмитрий Гусев
ОАО «ИнфоТеКС»
gusev@infotecs.ru