# Формирование Российской национальной инфраструктуры открытых ключей

(PKI, Public Key Infrastructure )

# Предпосылки развития инфраструктуры «электронного правительства»

- развитие сферы государственных услуг организациям и гражданам с использованием юридически значимого электронного документооборота;
- потребность государственных структур и бизнеса в организации межведомственного и межгосударственного юридически значимого защищенного электронного документооборота;
- развитие сферы электронной коммерции и ведения бизнеса на основе современных информационных технологий;
- появление на рынке развитых и доступных по цене средств, использующих технологии ЭЦП;
- наличие апробированной мировым сообществом практики применения ИОК;
- наличие средств ЭЦП отечественного производства, отвечающего требованиям современного уровня развития информационных технологий;
- появление на рынке информационно-коммуникационных услуг высококвалифицированных специалистов, организаций и компаний, ориентированных на деятельность в области защищенного документооборота, развития российской инфраструктуры ИОК.

# Инфраструктура открытых ключей решает следующие основные задачи:

- обеспечение конфиденциальности информации при ее хранении и передаче по открытым каналам связи за счет использования алгоритмов шифрования;
- обеспечение аутентификации, как пользователей, так и ресурсов, к которым обращаются пользователи;
- обеспечение невозможности отказа от совершенных пользователями действиях при обращении к информации;
- обеспечение целостности информации при ее хранении, обработке и передаче по открытым каналам связи за счет использования электронно-цифровой подписи (ЭЦП).

# Государственная политика в области использования ЭЦП в деятельности органов власти должна основываться на принципах:

- создание единого пространства доверия в части признания электронной цифровой подписи и сертификатов ключей подписи;
- согласованность нормативной правовой базы и методического обеспечения в сфере применения электронной цифровой подписи и информационных технологий на всех уровнях;
- консолидация бюджетных средств на создание и развитие систем удостоверяющих центров ОГВ.

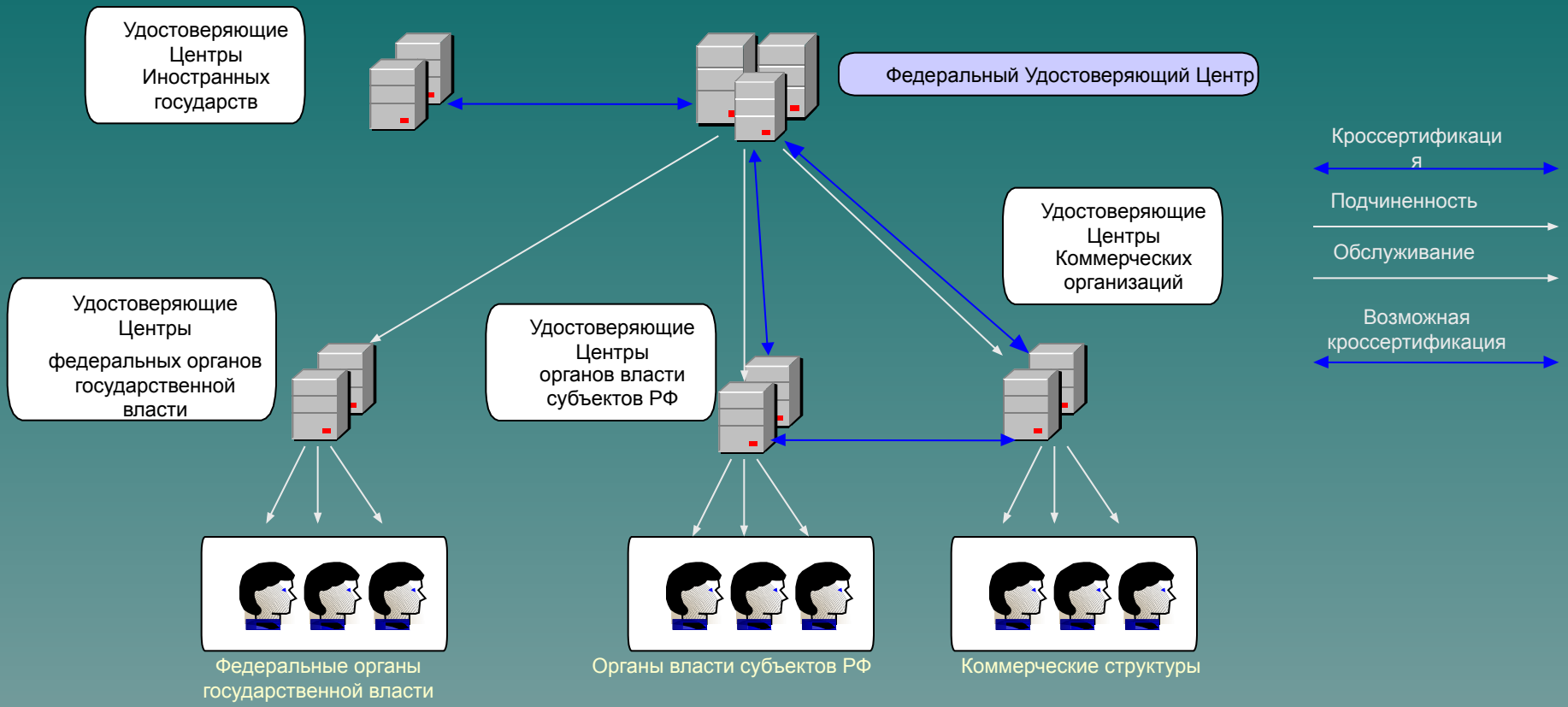
# Дополнительные подзаконные акты:

- закрепление функции Федерального УЦ за УФО;
- регламент исполнения функций уполномоченного федерального органа исполнительной власти в области использования ЭЦП;
- типовой регламент УЦ, формирование единого регламента СУЦ ОГВ;
- требования к органу государственной власти и органам местного самоуправления при работе с сертификатами ключей ЭЦП;
- рекомендации хозяйствующим субъектам по порядку хранения и использования закрытых ключей, применения ЭЦП, использования программно-аппаратных средств, обеспечения требуемой безопасности и использования средств защиты;
- порядок аккредитации удостоверяющих центров и контроля их деятельности;
- обеспечение финансовых гарантий деятельности и ответственности удостоверяющих центров;
- порядок сертификации (проверки соответсвия) средств ЭЦП;
- создание недостающего элемента информационной инфраструктуры России – Российского сегмента мирового пространства идентификаторов объектов и имен, построенного в соответствии с международными рекомендациями и практиками.

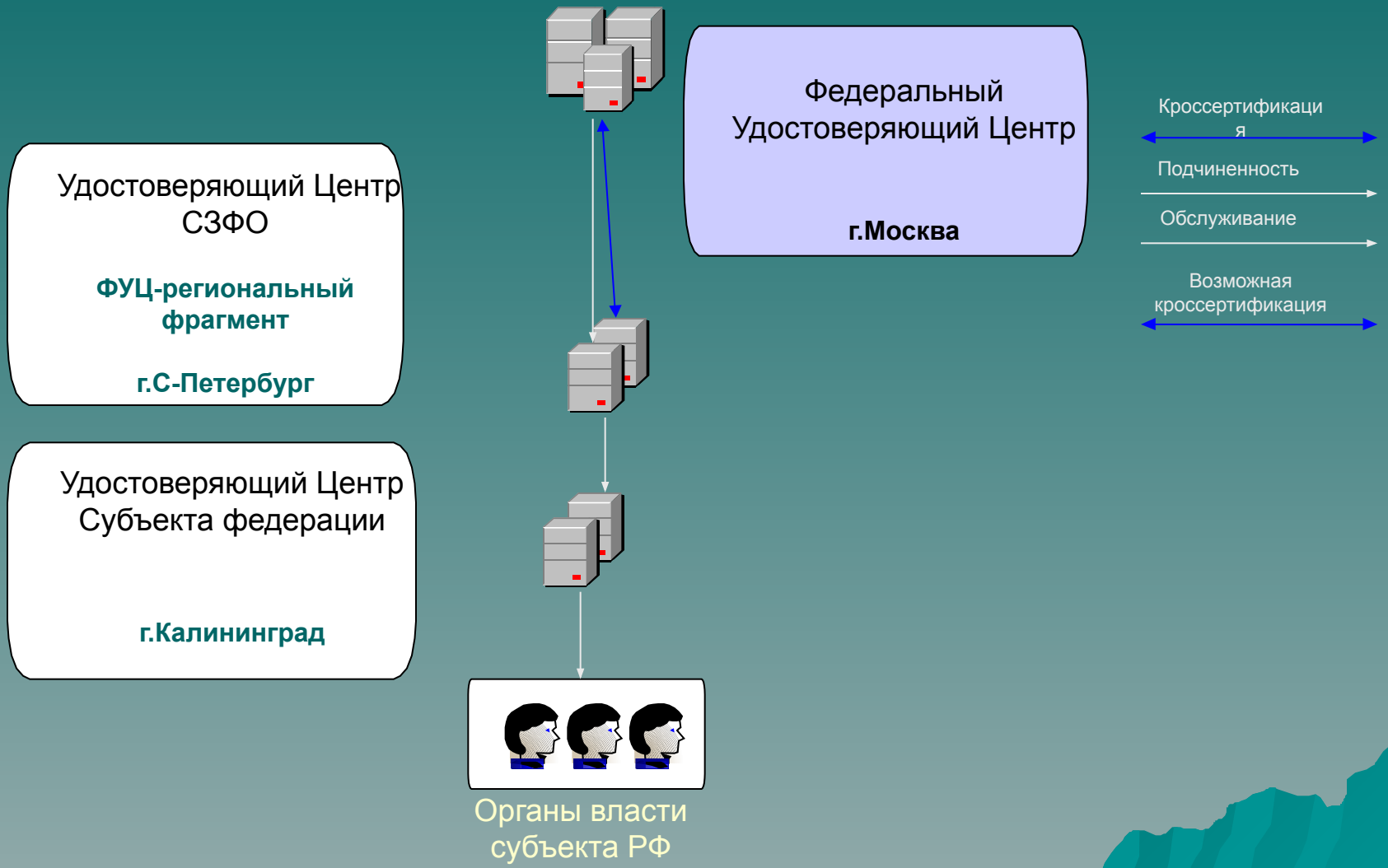
# Принципы построения СУЦ ОГВ:

- иерархичность структуры СУЦ ОГВ;
- единство политики безопасности СУЦ ОГВ;
- единство политик применения сертификатов ключей подписей;
- открытость системы для включения в ее состав новых УЦ при условии выполнения установленных требований;
- соответствие нормам действующего законодательства Российской Федерации в сфере применения ЭЦП и информационной безопасности;
- техническая совместимость используемых средств ЭЦП;
- уникальность используемых идентификаторов объектов, ключей и номеров сертификатов;
- аккредитация УЦ, как необходимое условие включения в систему.

# Архитектура СУЦ ОГВ



# Архитектура экспериментальной пилотной зоны



# Федеральный Удостоверяющий центр


**Технологической платформой ФУЦ является территориально-распределенный программно-аппаратный комплекс (ПАК), состоящий из центров сертификации и центров регистрации, прошедшими процедуру проверки соответствия средств ЭЦП.**

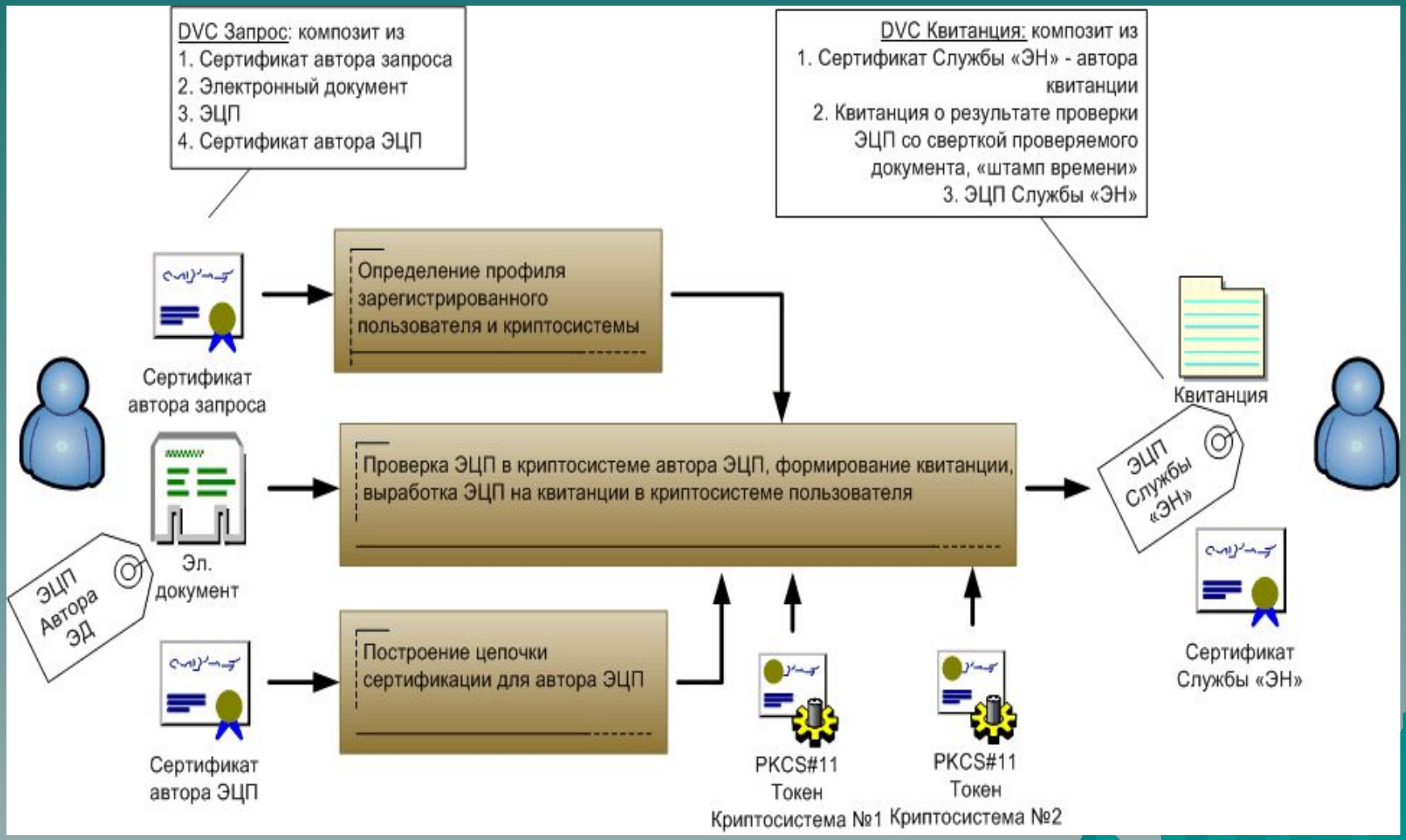
# Основные задачи по обеспечению информационной безопасности ФУЦ:

- защита конфиденциальной информации при ее хранении, обработке и передаче (персональные сведения, охраняемые в соответствии с действующим законодательством, парольная информация, информация аудита и т.п.);
- контроль целостности конфиденциальной и открытой информации: (информация о владельцах, входящая в состав сертификатов, информация об отозванных сертификатах, свободно распространяемые программные компоненты и документация к ним и т.п.);
- контроль целостности программных и аппаратных компонент комплекса;
- обеспечение безотказной работы.

# Подсистемы защиты информации в ФУЦ

- подсистема криптографической защиты информации, включающая в себя программные и/или программно-аппаратные СКЗИ;
- подсистема защиты информации от несанкционированного доступа (НСД);
- подсистема активного аудита информационной безопасности УЦ;
- подсистема обнаружения вторжений;
- подсистема резервного копирования и архивирования данных;
- подсистема обеспечения целостности информации, программных и аппаратных компонент комплекса, в том числе криптографическими методами;
- подсистема обеспечения безотказной работы комплекса, включающая в себя регулярно обновляемые антивирусные средства;
- подсистема защиты оборудования комплекса от утечки информации по техническим каналам и побочным ЭМИ;
- подсистема обеспечения защиты информации от НСД организационными, режимными и техническими методами.

# Структурная схема Службы «Электронного нотариата»

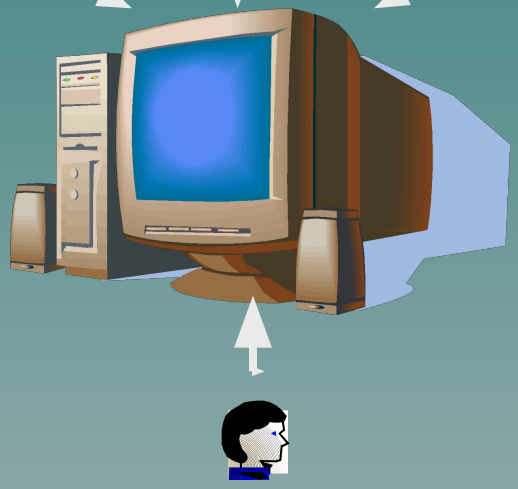


# Инфраструктура «одного окна»

Орган государственной власти 1

Орган государственной власти 2

Орган государственной власти 3



«Единое окно»

Гражданин

# Благодарю за внимание!

Голобоков Владимир Анатольевич
Начальник отдела реестров СКП
РОСИНФОРМТЕХНОЛОГИИ
(495) 771-85-39
e-mail: rufo@minsvyaz.ru