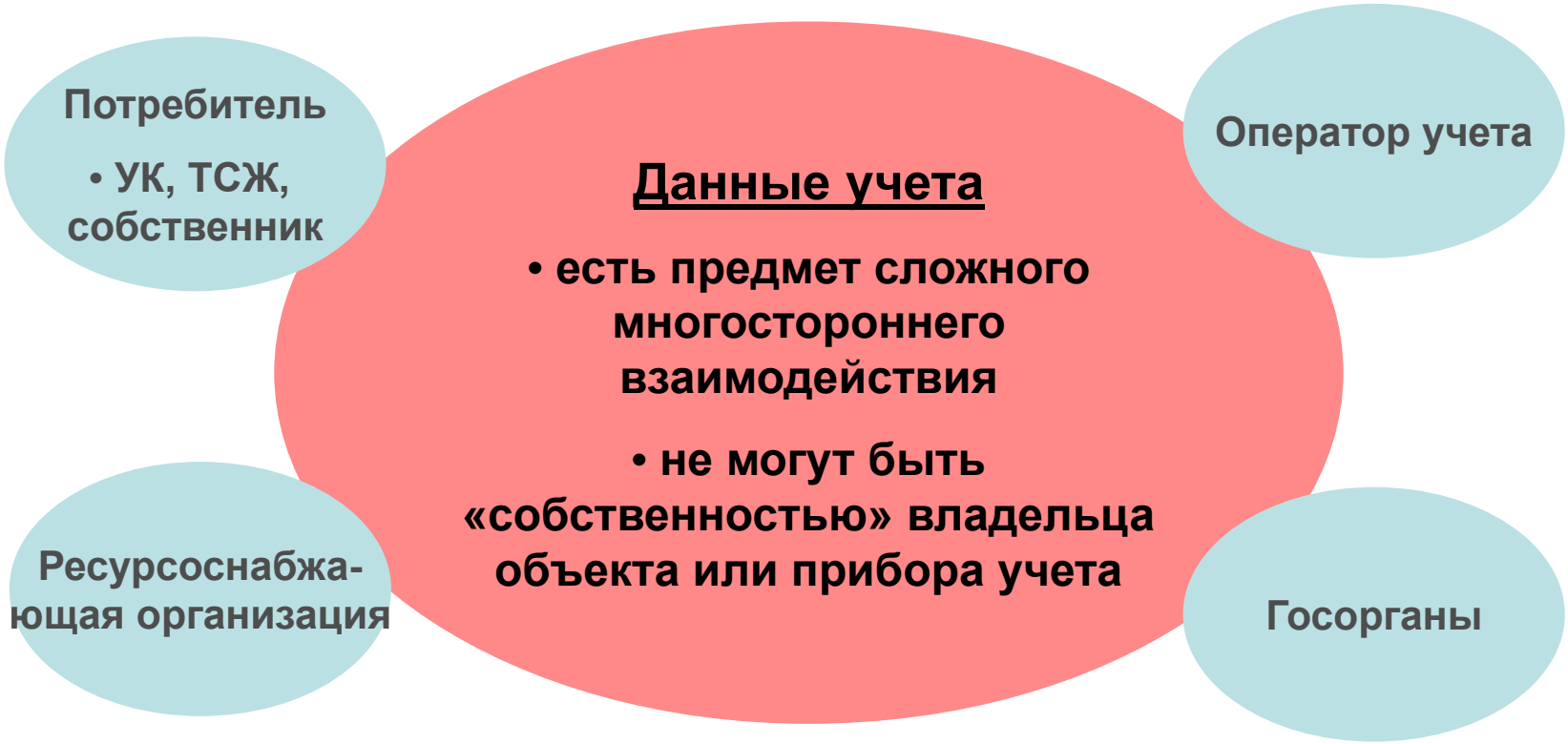
ТЕХНОЛОГИЧЕСКИЙ ДОКУМЕНТООБОРОТ

ДЛЯ УЧЕТА ПОТРЕБЛЕНИЯ РЕСУРСОВ

Докладчик: Ледовский С.Д. – Генеральный директор ООО НПО Карат



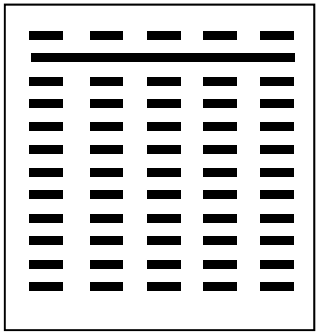
ПРОБЛЕМЫ, ЗАДАЧИ:

- Прозрачность
- достоверность
- Надежность
- Юридическая значимость

«ИЗМЕРИТЕЛЬНАЯ СИСТЕМА»

«ПРОДУКТ»

отчет, принятый ресурсоснабжающей организацией



ВОПРОС:

Измерение или передача данных?

Обстоятельства формирования технологии:

- Проблемы законодательства
- Проблемы коммуникаций и связи
- Слабые процессоры для автономных устройств

Что изменилось сейчас:

- Новый закон «Об электронной подписи»
- Мощные, дешевые и экономичные ARM-процессоры с поддержкой Linux
- Облачные технологии, интернет-сервисы
- Доступные коммуникации: плотность сети, дешевые компоненты, упрощение радиорегулирования

Научно-Производственное Объединение КАРАТ

Прозрачность, достоверность, юридическая значимость:

- **ТЕХНИЧЕСКИМИ СРЕДСТВАМИ**
- **БЕЗ УЧАСТИЯ ЧЕЛОВЕКА**

Функции объектового сервера

- Функции вычислителя, коммуникатора, пульта «в одном флаконе»
- База данных показаний приборов и средства взаимодействия со «старыми» системами диспетчеризации для совместимости
- Средства криптозащиты, электронной подписи, защищенных коммуникаций, ключи
- Архив официальных отчетов с электронной подписью

Функции облачного сервиса

- «Ведомственный» удостоверяющий центр электронных подписей
- Реестр узлов учета, объектовых серверов, объектов, приборов учета, пользователей
- Архив дубликатов официальных отчетов
- Центр управления и мониторинга объектовых серверов

Электронная подпись

ЗАКРЫТЫЙ КЛЮЧ

Можно вычислить →

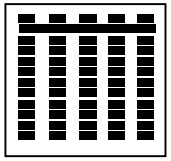
← Невозможно вычислить

ОТКРЫТЫЙ КЛЮЧ

Держу в тайне

Раздаю контрагентам или публикую для всех

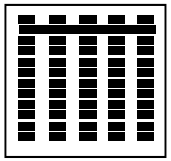
Подписание документа

Шифрую закрытым ключом →  →

Расшифровывают открытым ключом, значит, шифровал я – закрытый ключ только у меня

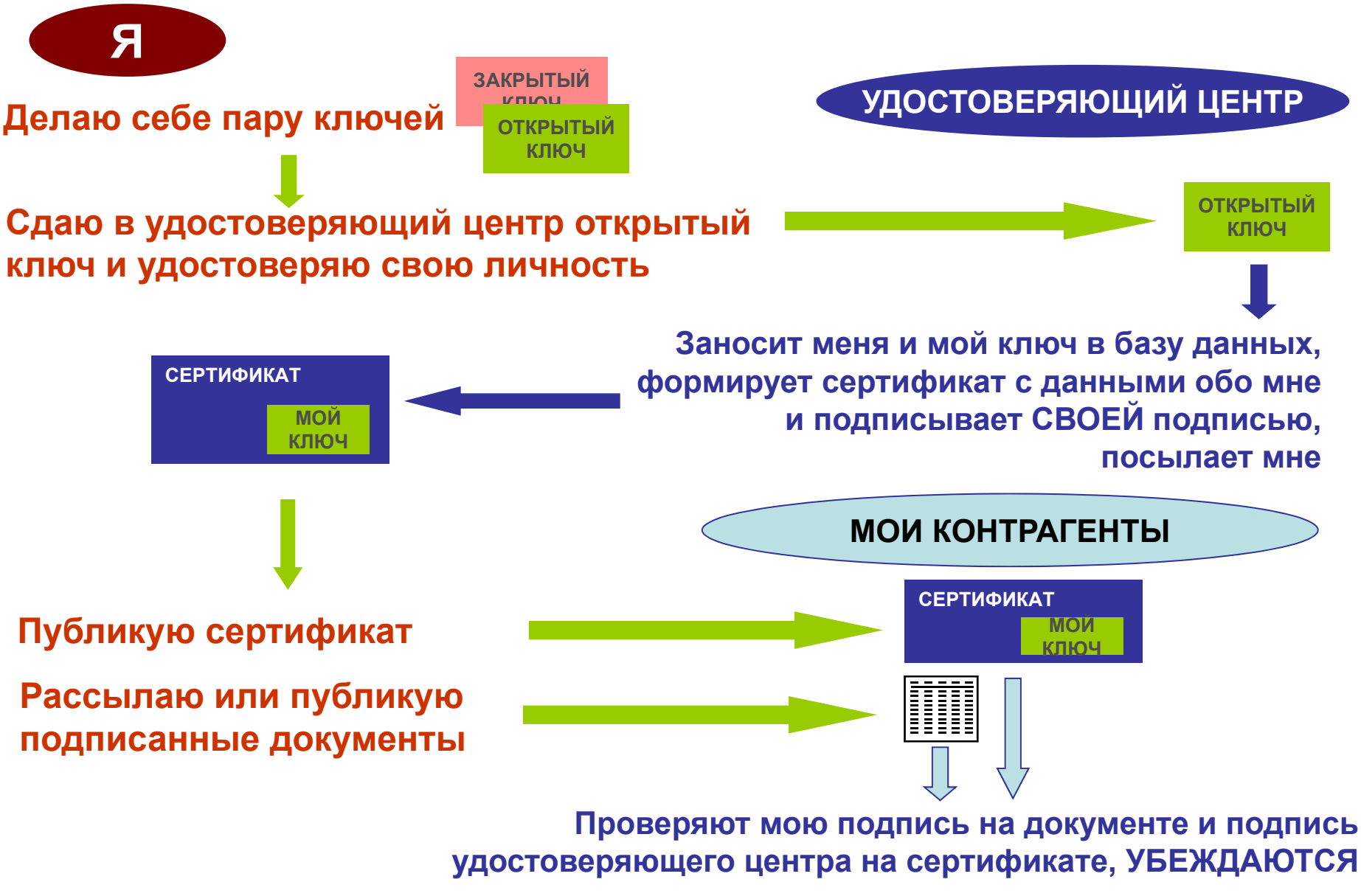
Шифрование документа для отправки мне

Закрытый ключ только у меня – прочитать могу только я ←



← Шифруют открытым ключом, расшифровать можно только закрытым ключом

Сертификат электронной подписи



Реализация в объектовом сервере

В процессе производства:

- В устройство – «объектовый сервер» прошиваются ключ основной электронной подписи, ключ и другие параметры защищенного канала в облачный сервис
- Устройство и его ключи регистрируются в реестре облачного сервиса, формируется сертификат основной электронной подписи устройства
- Генерируется код доступа в облачный сервис для будущего владельца объектового сервера

В процессе монтажа и пусконаладки узла учета:

- Владелец узла учета и объектового сервера регистрируется в облачном сервисе с помощью кода доступа
- Владелец формирует средствами сервиса (самостоятельно или с помощью оператора учета) параметры узла учета и параметры эксплуатации объектового сервера
- Параметры загружаются в объектовый сервер через центр управления сервиса

В процессе эксплуатации узла учета:

- Объектовый сервер опрашивает приборы учета, формирует и подписывает официальные отчеты, отправляет дубликаты отчетов в архив сервиса
- Сервис выполняет автоматический контроль целостности и защиты объектового сервера, обновляет ключи и сертификаты по необходимости

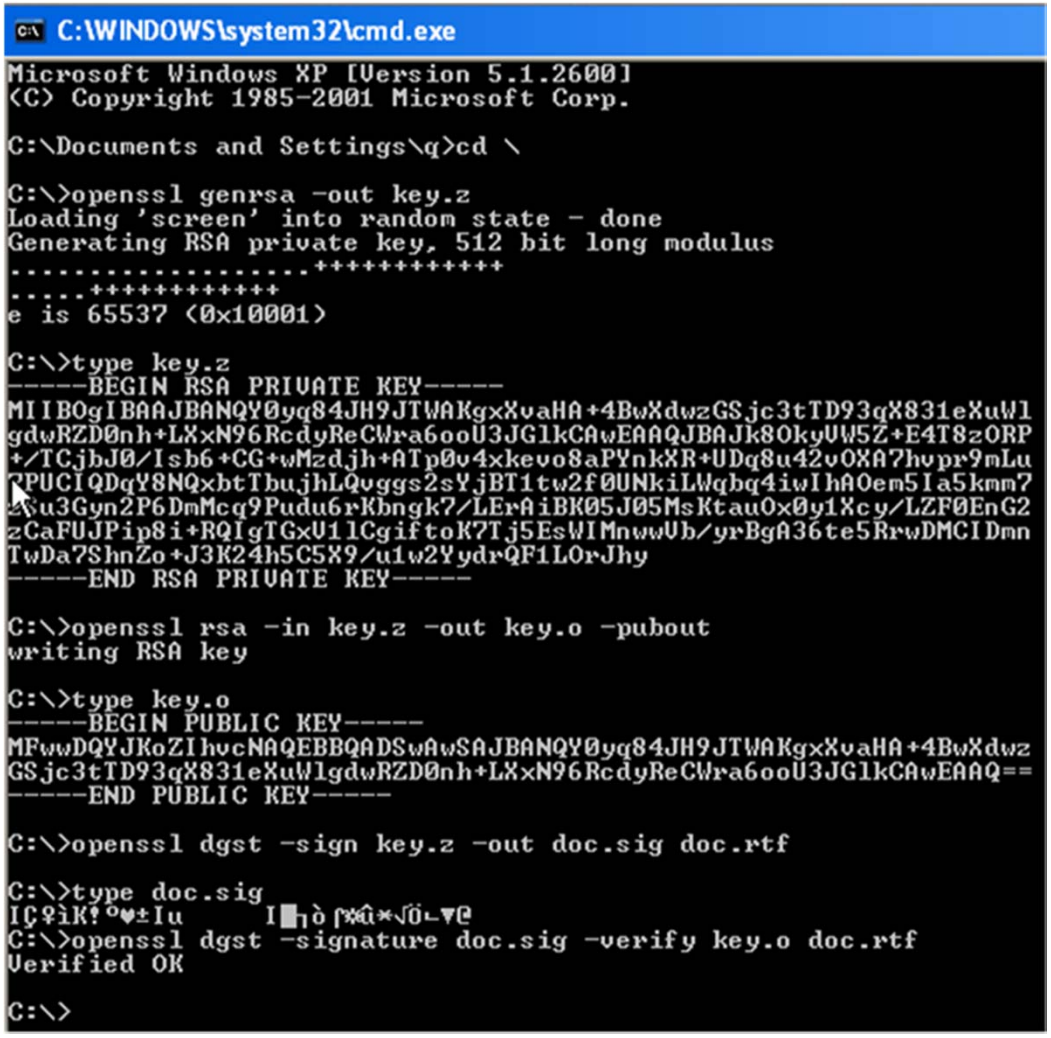
Средства реализации

OpenSSL – открытая библиотека криптозащиты, фактический стандарт:

- Бесплатная, открытая, свободно распространяемая в исходных кодах
- Реализована для всех распространенных операционных систем, в том числе для ОС Linux в версиях для процессоров ARM, применяемых в объектовом сервере
- Содержит все необходимые алгоритмы шифрования, включая ГОСТ
- Безопасность, обнаружение и оперативное устранение уязвимостей, отсутствие скрытой функциональности контролируется мировым независимым сообществом разработчиков библиотеки

Работа с OpenSSL - пример

Используем утилиту командной строки openssl.exe



Сделали закрытый ключ (положили в файл key.z)

Посмотрели закрытый ключ (просто интересно)

Сделали открытый ключ

Посмотрели открытый ключ (файл key.o)

Подписали файл doc.rtf

Посмотрели подпись (файл doc.sig)

Проверили подпись - ОК

Работа с OpenSSL - пример

```
C:\>openssl req -x509 -new -key key.z -config ssl.cfg -out key.crt -days
Loading 'screen' into random state - done

C:\>type key.crt
-----BEGIN CERTIFICATE-----
MIICFjCCAcACCQD7GyL7d/cE6TANBgkqhkiG9w0BAQUFADCBkTEWMBQGA1UECBMN
U3ZlcmRsb3Zza2F5YTEVMBMGA1UEBxMMRWthdGUyaW5idXJnMQ4wDAYDVQQKEwVL
YXJhdDEMMAoGA1UECxMDT1BQMRkwFwYDVQQDExBBbGV4ZWkgU2l2ZW50c2V2MScw
JQYJKoZIhvcNAQkBFhhjZXJ0aWZpY2F0ZUBrYXJhdC1ucG8ucnUwHhcNMTIxMjE5
MTEyMjMwWhcNMTMxMjE5MTEyMjMwWjCBkTEWMBQGA1UECBMNU3ZlcmRsb3Zza2F5
YTEVMBMGA1UEBxMMRWthdGUyaW5idXJnMQ4wDAYDVQQKEwVLYXJhdDEMMAoGA1UE
CxMDT1BQMRkwFwYDVQQDExBBbGV4ZWkgU2l2ZW50c2V2MScwJQYJKoZIhvcNAQkB
FhhjZXJ0aWZpY2F0ZUBrYXJhdC1ucG8ucnUwXDANBgkqhkiG9w0BAQEFAANLADBI
AkEA1BjTKrzgkf01NYAqDFe9ocD7gHBd3DMZKNze1MP3epfzfV5e5aWB3BFkPSeH
4tfE33pFx3JF4JatrqihTckaWQIDAQABMA0GCSqGSIb3DQEBBQUAA0EAmgNbBaeX
ykI4Hv0Lzf98AzYiZE7GT5jX7L4/oiG+Ug6/IIQGDUtLeZKXzGH3psdeQJHLsFau
nGMeebTln3et1A==
-----END CERTIFICATE-----

C:\>openssl x509 -in key.crt -noout -text
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            fb:1b:22:fb:77:f7:04:e9
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: ST=Sverdlovskaya, L=Ekaterinburg, O=Karat, OU=NPP, CN=Ale
entsev/emailAddress=certificate@karat-npo.ru
        Validity
            Not Before: Dec 19 11:22:30 2012 GMT
            Not After : Dec 19 11:22:30 2013 GMT
        Subject: ST=Sverdlovskaya, L=Ekaterinburg, O=Karat, OU=NPP, CN=Al
ventsev/emailAddress=certificate@karat-npo.ru
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (512 bit)
                Modulus:
                    00:d4:18:d3:2a:bc:e0:91:fd:25:35:80:2a:0c:57:
                    bd:a1:c0:fb:80:70:5d:dc:33:19:28:dc:de:d4:c3:
                    f7:7a:97:f3:7d:5e:5e:e5:a5:81:dc:11:64:3d:27:
                    87:e2:d7:c4:df:7a:45:c7:72:45:e0:96:ad:ae:a8:
                    a1:4d:c9:1a:59
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        9a:03:5b:05:a7:97:ca:42:38:1e:fd:0b:cd:ff:7c:03:36:22:
        64:4e:c6:4f:98:d7:ec:be:3f:a2:21:be:52:0e:bf:20:84:06:
        0d:4b:4b:79:92:97:cc:61:f7:a6:c7:5e:40:91:cb:b0:56:ae:
        9c:63:1e:79:b4:e5:9f:77:ad:d4
```

Сделали сертификат (положили в файл key.crt)

Посмотрели, что в файле сертификата (просто интересно)

Вывели содержание сертификата на экран в текстовом виде

Все необходимые операции с ключами, сертификатами и подписями доступны через простые команды в командной строке (в Windows, Linux, MacOS одинаково)

Контактная информация

ГОЛОВНОЙ ОФИС в ЕКАТЕРИНБУРГЕ:

Екатеринбург, ул. Ясная, 22 корп. Б; т./ф.:(343) 22-22-307, 22-22-306

МОСКОВСКИЙ ФИЛИАЛ:

Москва, ул. Большая Марьинская, 9, стр1, оф.9 т./ф.:(495) 280-10-24

СИБИРСКИЙ ФИЛИАЛ:

Новосибирск, ул. Добролюбова, 12; т./ф.:(383) 269-34-35, 206-34-35

ЮЖНО-УРАЛЬСКИЙ ФИЛИАЛ:

Челябинск, ул. Грибоедова, 57 корп. А; т./ф.:(351) 729-99-04

ЗАПАДНО-УРАЛЬСКИЙ ФИЛИАЛ:

Пермь, ул. Кронштадтская, 39 корп. А; т./ф.:(342) 257-16-04

ВОЛГОГРАДСКИЙ ФИЛИАЛ:

Волгоград, ул. Калинина, 13; т./ф.:(8442) 60-03-76

ДАЛЬНЕВОСТОЧНОЕ ПОДРАЗДЕЛЕНИЕ:

Владивосток, Партизанский проспект, 58, оф.6.2; т./ф.:(423) 245-28-28

ВОСТОЧНО-СИБИРСКОЕ ПОДРАЗДЕЛЕНИЕ:

Красноярск, ул. Телевизорная, 1, стр.4; т./ф.:(391) 223-23-13

КАРАТ-ПОВОЛЖЬЕ:

Чебоксары, Марпосадское шоссе, 1 «Б»; т./ф.:(8352) 32-01-82

СПАСИБО ЗА ВНИМАНИЕ!

www. karat-npo.ru