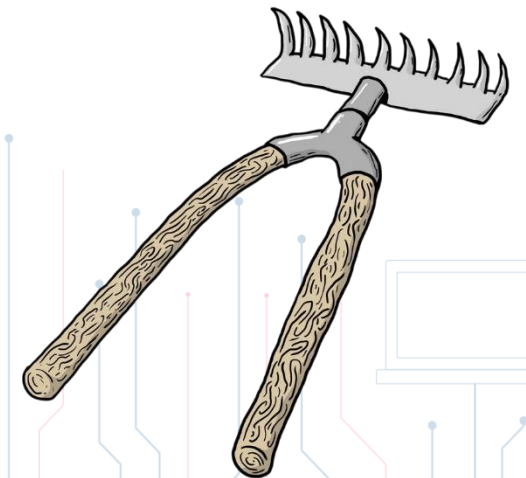


# Грабли клиентской аутентификации

И как мы обошли их, разрабатывая TLS VPN шлюз  
**КриптоПро NGate**

Александр Никитков  
**КриптоПро**



Там и тут..





# С чем обычно приходит заказчик?



сертификат?

логин\пароль?

одноразовые пароли  
(MFA)?

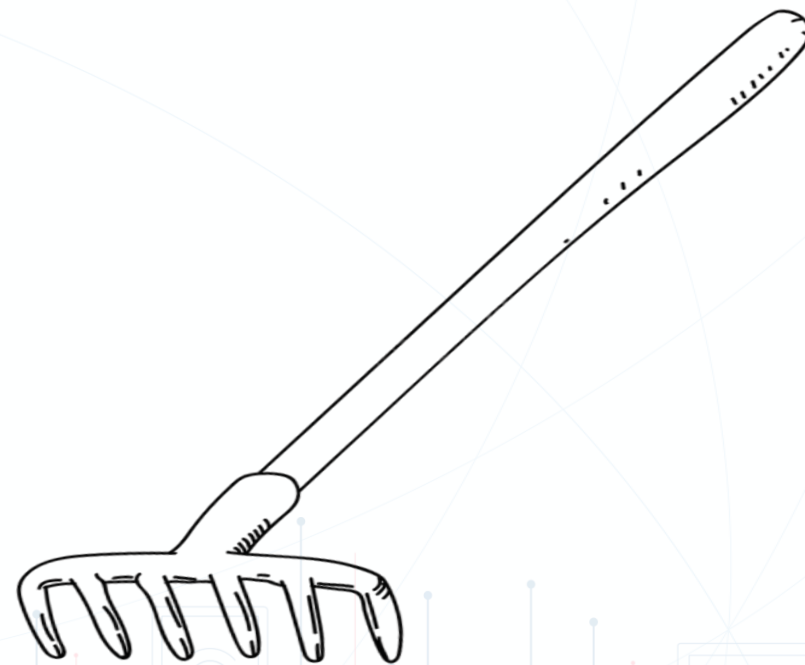


# Аутентификация по логину\паролю



Используем данные из служб каталогов, а не из локальной БД пользователей.

- Как единственный тип - не годится
- Учётку в **LDAP** легко заблокировать
- Взаимодействие с **LDAP** напрямую – харам!





Разворачиваем PKI, если таковая отсутствует.



# Грабли сертификатного доступа



- Хороший **PKI** - недешевое удовольствие
- Ограничение доступа на основе **CRL** – вещь не быстрая
- “Голый” **OCSP** не пойдёт,  
а **OCSP stapling** ещё надо суметь..

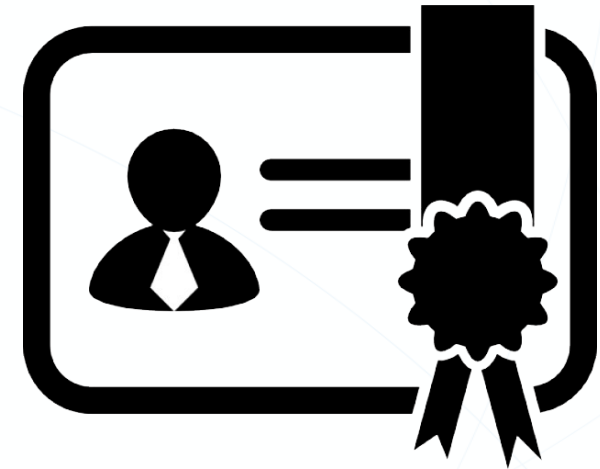




# А что, если сертификат квалифицированный?

---

- Как запретить доступ пользователю?
- Куча личных данных в сертификате!
- А что там, на другой стороне?





Точечно управляем доступом пользователей!

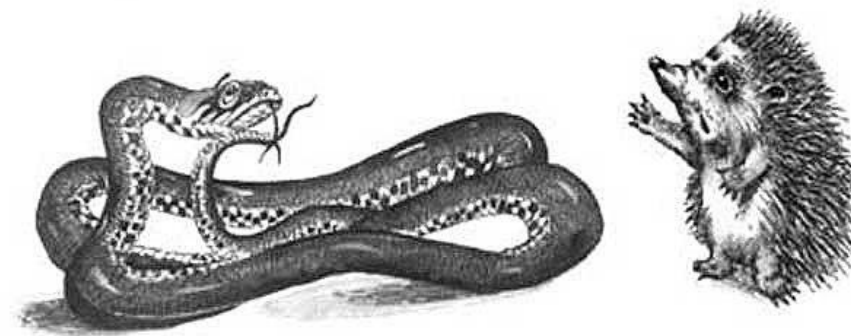
И не только сертификатным...



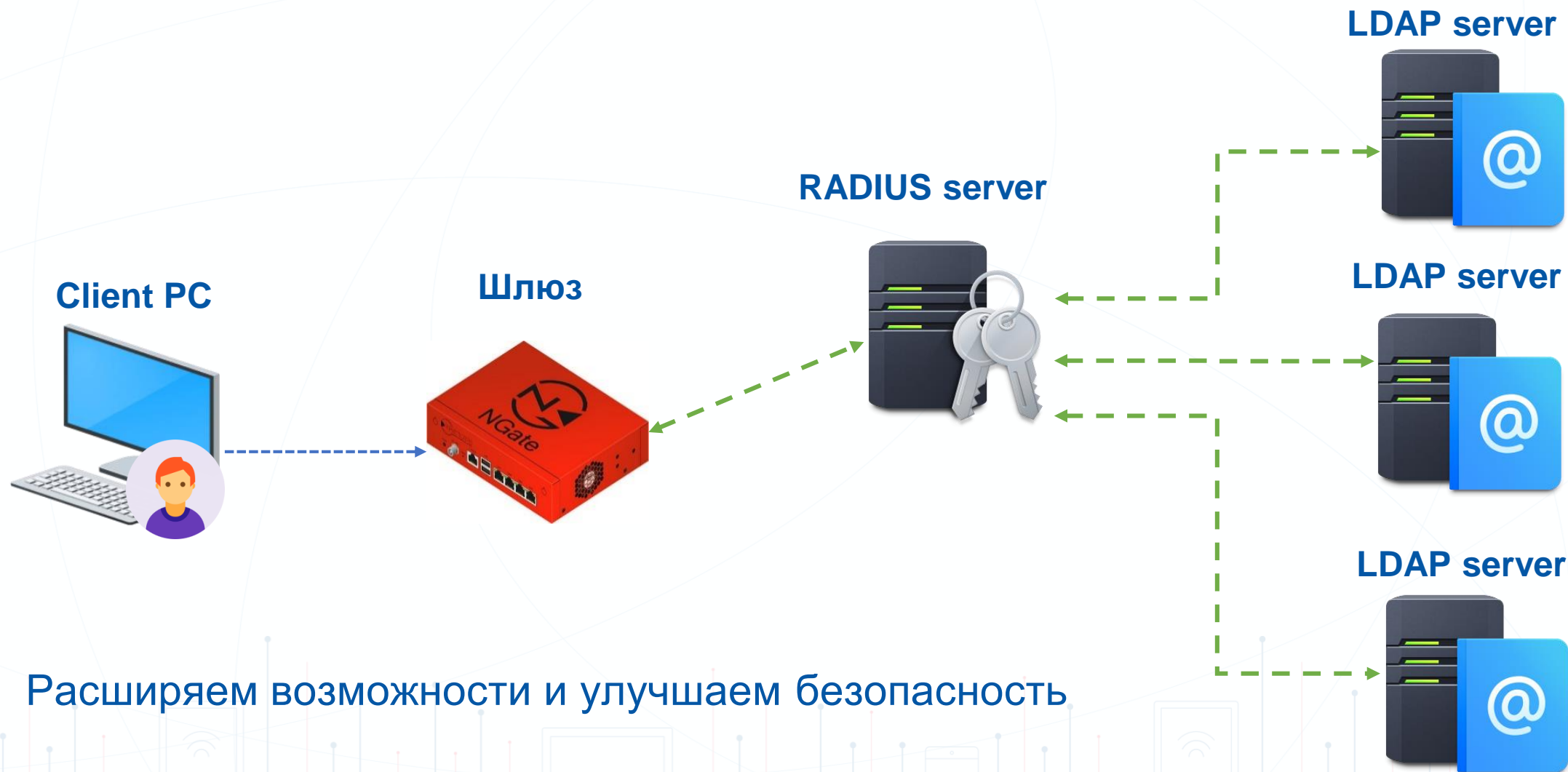
# Что если скрестить ежа с ужом объединить оба типа?

---

- Сертификат **и** LDAP
- Сертификат **в** LDAP
- Сертификат **с UPN в** LDAP (AD)



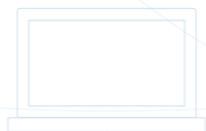
# Добавляем RADIUS сервер!



# Преимущества использования RADIUS



- Поиск единовременно во множестве **LDAP**
- Функционал **MFA (TOTP/HOTP/etc.)**
- Существенное расширение возможностей аутентификации (**VSA** и т.д.)



# Какие ещё схемы аутентификации имеются?

- Комбинации из всего перечисленного ранее!
- + Ограничение доступа по дате и времени
- + Дискриминация по гео.признаку :)

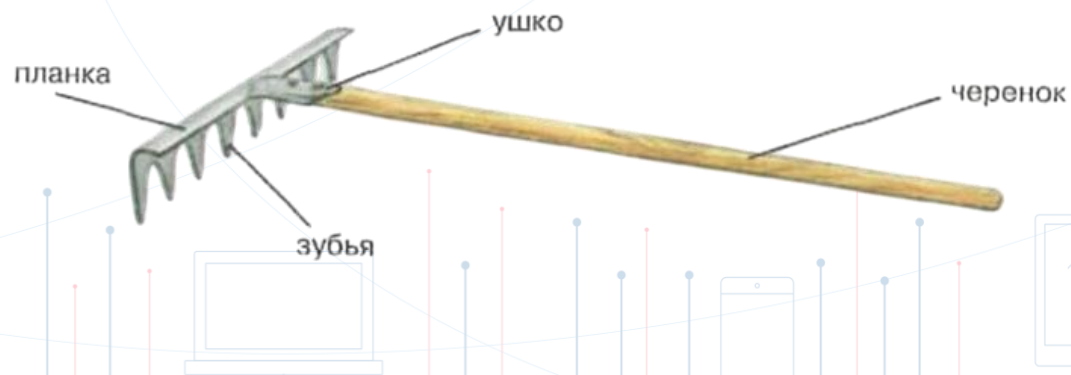


# Что в итоге?



Реализуем проверенное, добавляем своё, обходим грабли, и

**комбинируем!**







**Ключевое слово  
в защите информации**

**СПАСИБО ЗА ВНИМАНИЕ!**



**Форма для отзывов:**



127018, г. Москва, ул. Суцеский Вал, д.18  
Тел./факс: +7 (495) 995-48-20

<https://cryptopro.ru>  
[alexandern@cryptopro.ru](mailto:alexandern@cryptopro.ru)  
[ngate@cryptopro.ru](mailto:ngate@cryptopro.ru)