«Single Sign-On» (SSO) at JINR.

Аутентификация - процесс проверки личности с помощью некой уникальной информации , в нашем случае с помощью имени входа и пароля.

Авторизация - это проверка и определение полномочий на выполнение некоторых действий (чтение-запись, доступ к ресурсам , управление) в соответствии с ранее выполненной аутентификацией

BATCH system : pbspwstore

afs : fs la , fs sa

sudoers определенные пользователи могут запускать команды под root без необходимости пароля root.

Аутентификация (+авторизация) ЦИВК + ГРИД +Облачная структура:

Kerberos + ldap ; voms + certifications.

Kerberos - сетевой протокол аутентификации

- идентификацией и аутентификацией пользователей;
- защита передаваемых сообщений.

  TGS— ticket granting server .

  klist, tokens (kinit , aklog)

Идентификация — распознание , установление тождественности неизвестного объекта известному на основании совпадения признаков.

***LDAP —** протокол, использующий TCP/IP и позволяющий выполнять операции аутентификации (bind), поиска (search) и сравнения (compare), а также операции добавления, изменения или удаления записей. (Гремучая смесь стандартизированного протокола и базы данных + средства управления)*

***LDAP + Kerberos** отличная комбинация:*

Kerberos используется для безопасного управления учетными данными (аутентификация), LDAP используется для хранения информации об учетных записях (полное имя, идентификатор, группы пользователя) .

«Single Sign-On» (SSO) .

опытная единая система аутентификации пользователей

NOC — А. Долбилов В.Чурин В.Фарисеев

Доступ в личный кабинет через sso логин-пароль :

- **регистрацию на ферме ЛИТ** *(использовавние ресурсов)*
- *системных администраторов своей Лаборатории*
- *Сетевой службе ОИЯИ (ЛИТ, к.216, тел.6-34-88,* **noc@jinr.ru***)*

После завершения регистрации вход в личный кабинет :
http://login.jinr.ru

- подтвердить почтовый адрес ,
- изменить/добавить почтовый адрес,
- изменить пароль для своей учетной записи

Доступ : (Jinrid)

pin.jinr.ru, disk.jinr.ru, базе документов ОИЯИ, ADB2, СЕД .

Удобства :

1. одна и та же учетная запись для доступа к нескольким приложениям

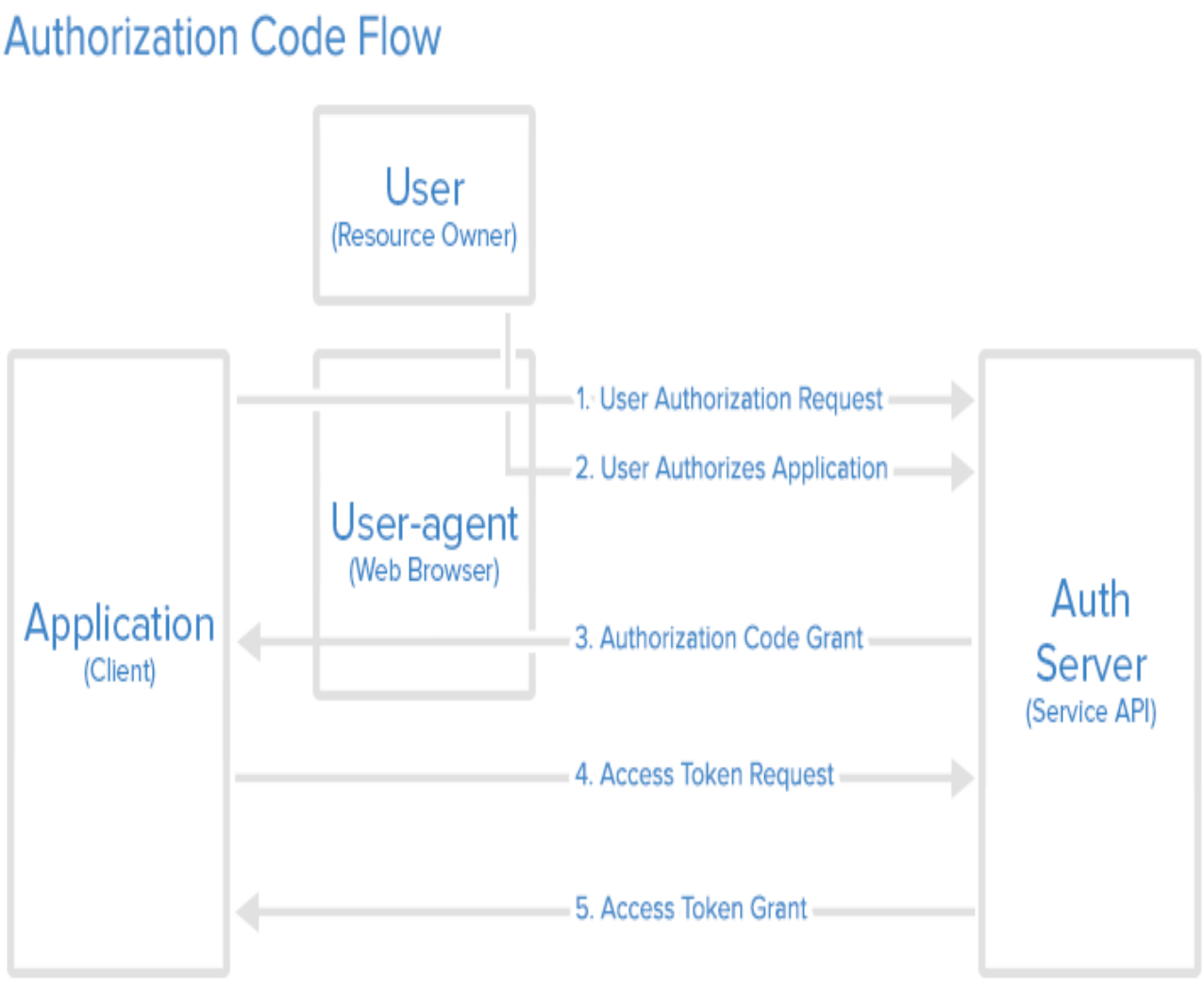
2. простое изменение пароля

3. способ снизить риск несанкционированного доступа, поскольку пароли не хранятся в системе.

4. единая система аутотентификации не создаст совпадений-путаницы
…
(sso<----> lxpub.jinr.ru)

Oauth 2.0

Protocol Flow & Grant Type: Authorization Code (token)



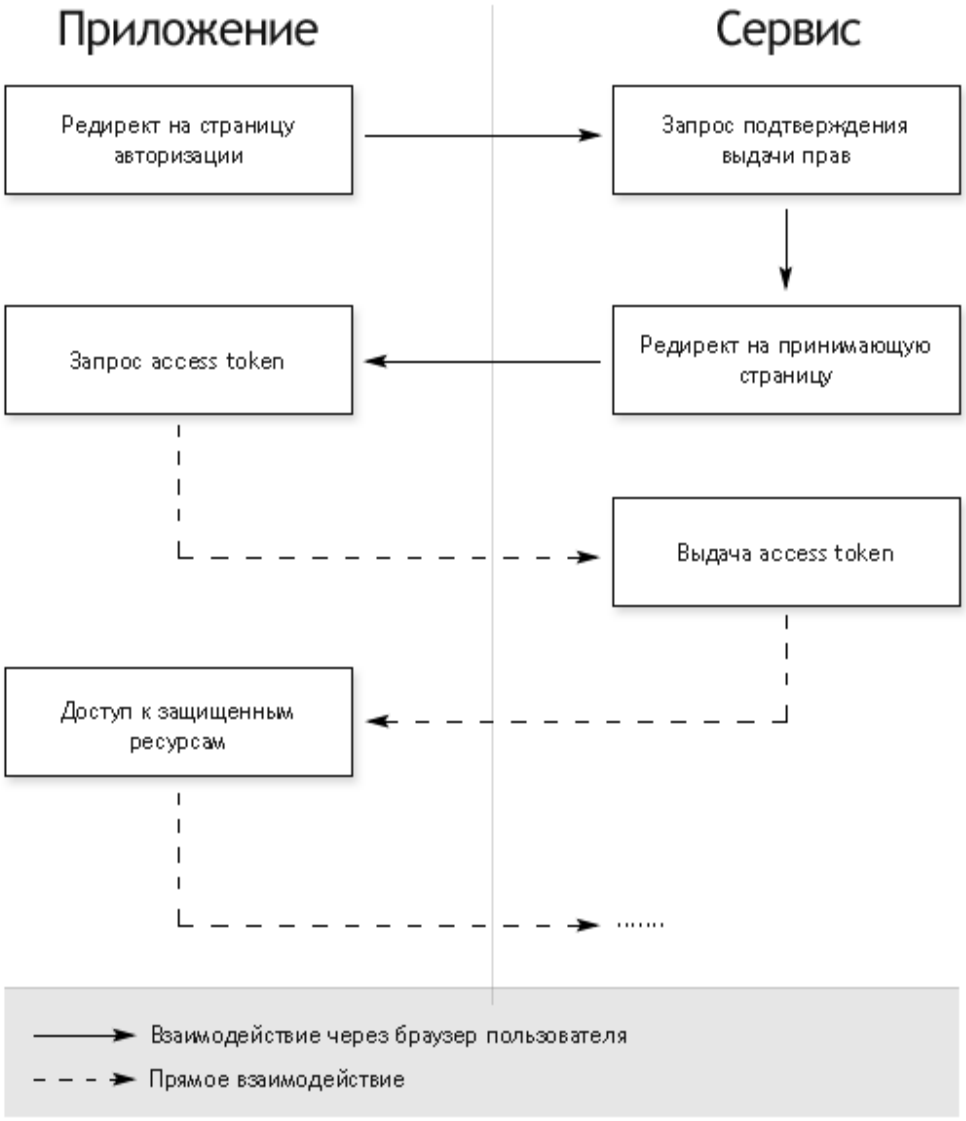
http://pin.jinr.ru

http://disk.jinr.ru

http://baza.jinr.ru

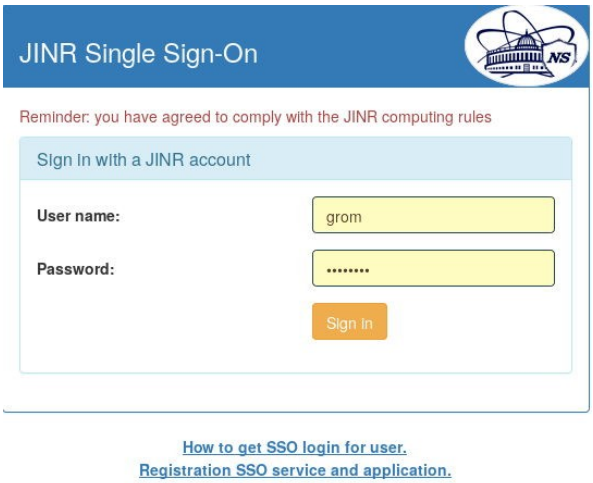
http://*login.jinr.ru* *(SSO пароль)*

http://sed.jinr.ru



Login.jinr.ru

I. для пользователей



II. для администраторов
admin,
name/admin@jinr.ru
(сервер аутотенфикации Oauth2.0):

- *редактировать учетные записи*
- *добавлять/удалять пользователей (БД ОИЯИ, ЦИВК (krb5+ldap))*
- *менять пароли*
- *добавлять/регистрировать web-apps (id, passwd ...)*

Аутентификация Авторизация МИВК
(Kerberos + ldap ; voms + certifications) :

I. *ЦИВК, ГРИД , Облачная структура*
II. *HybriLIT - свой Kerberos + ldap*

Единая Аутентификация МИВК *:*

1. ЦИВК ldap + HybriLIT ldap

2. kerberos = один общий (?)

Аутотенфикации/регистрации через SSO.

1. ***ТОЛЬКО*** сотрудники ОИЯИ (управление) (JINRid+kerberos)
2. доступ только к ***web-приложениям*** *---> Сетевая служба (kerberos)*
3. доступ к ***счетным ресурсам/ресурсам хранения*** *--->*

Заявка на регистрацию *LXPUB (kerberos,ldap,afs)*

ОИЯИ+ Не ОИЯИ

Единая аутотенфикация ОИЯИ использует:

- *БД управления ОИЯИ — ФИО*, JINRid, место работы
- *kerberos (username)*
- *ldap (username, uidNumber, gidNumber, Name and Surname laboratory ...)*

Некоторые трудности :

- нет соответствия базы ОИЯИ и ldap (*Name and Surname не = ФИО)*

  (новые пользователи ЦИВК : логин-латиница, а ФИО — кириллица)
- пользователь может быть:

1. только в kerberos
2. kerberos ldap afs — но не сотрудник ОИЯИ (не давать доступ к SSO)

- пользователи Гетерогенная Платформа/Говорун - другой kerberos

Варианты:

- username <=8 символов: ---> единый логин к SSO и LXPUB
- username > 8 символов : ---> разные учетные записи на LXPUB и SSO

Вывод:

Сервис SSO и Сервис User Accounting

не обязательно должны быть связаны .

Single Sign On and Account Management Services

Services responsible for user authentication on central machines managed by IT:

- The Single Sign-On service provides a solution allowing Web based applications to authenticate users and retrieve their information including their group membership to manage authorizations.

- The Account Management Service (formerly known as FIM) provides all the tools to centrally manage computer accounts and resource authorization for end users, supervisors, the service desk and security team.