# Сигурност, упълномощаване и удостоверяване

***Mike Mineter***

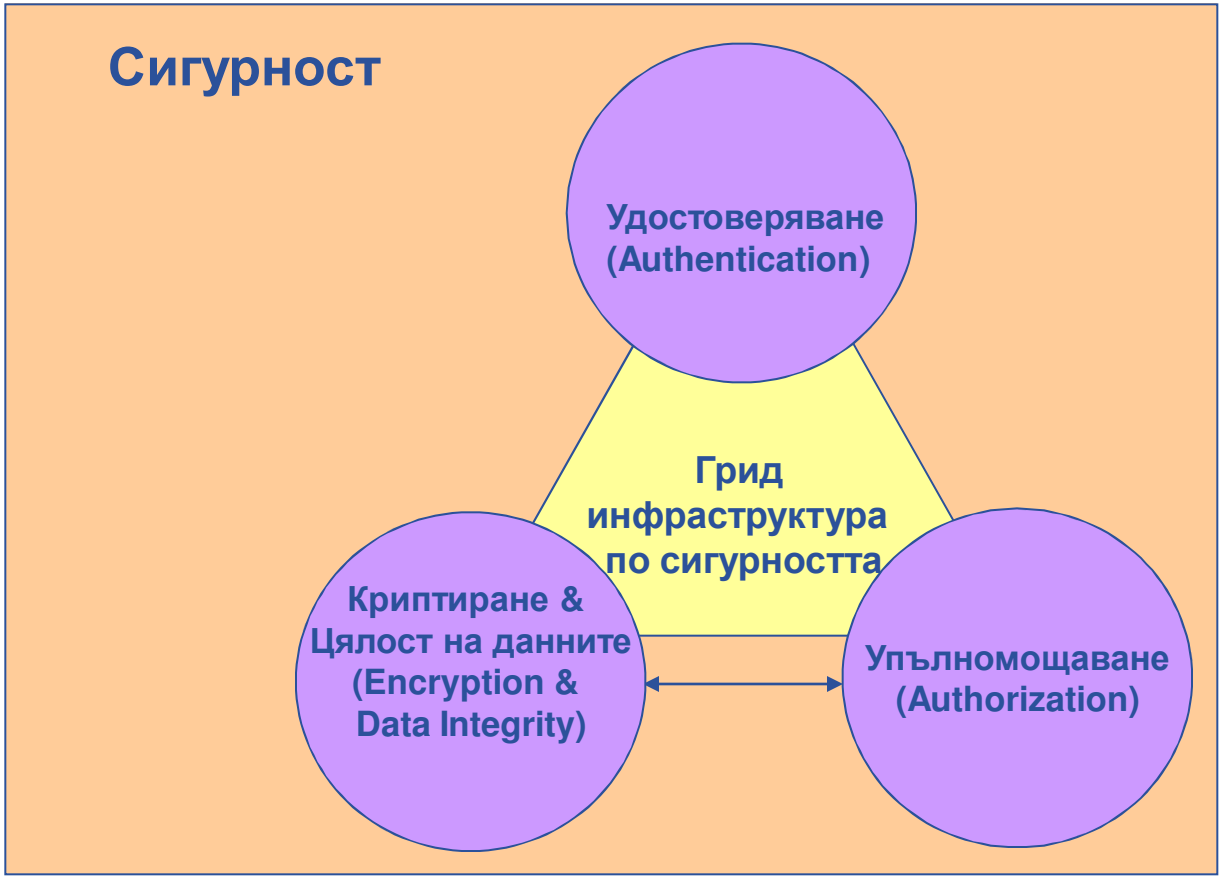
***Training, Outreach and Education***

***National e-Science Centre***

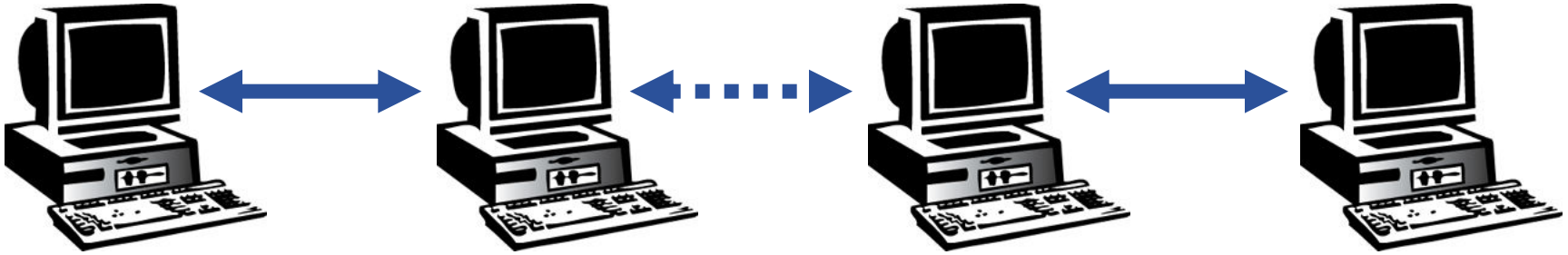
***mjm@nesc.ac.uk***

***С благодарности за някои от слайдовете към колегите от EGEE и Globus***

# Преглед на сигурността



# Проблемите - 1



**Потребител** **Ресурс**

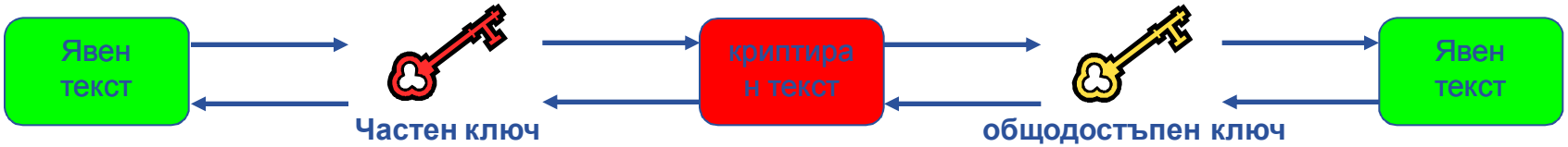
- **Как Потребителят получава сигурен достъп до Ресурса без да има регистрация с потребителско име и парола на машините помежду им, а даже и на машината, където е ресурса?**
- **Как Ресурса знае кой е Потребителя?**
- **Как се контролират правата?**

**Удостоверяване:** **как се предава идентичността на потребителя/сайта?**

**Разрешение за достъп:** **какво може да прави потребителя?**

# Основи на сигурността & удостоверяване

- **Асиметрично криптиране…**



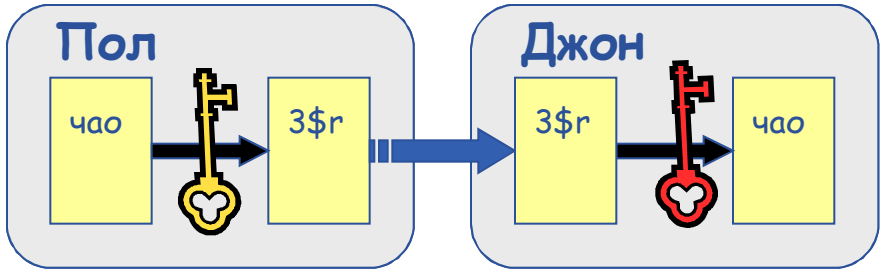

- **…. и Цифрови подписи …**
  - Хеш, извлечен от съобщението и криптиран с частен ключ на подписващия
  - Подписа се проверява с декриптиране чрез общодостъпния ключ на подписващия

- **За изграждане на доверие**
  - Потребителят / сайта са тези, за които се представят
  - Може да им се има доверие в съответствие с уговорените политки

# Алгоритми с общодостъпни ключове

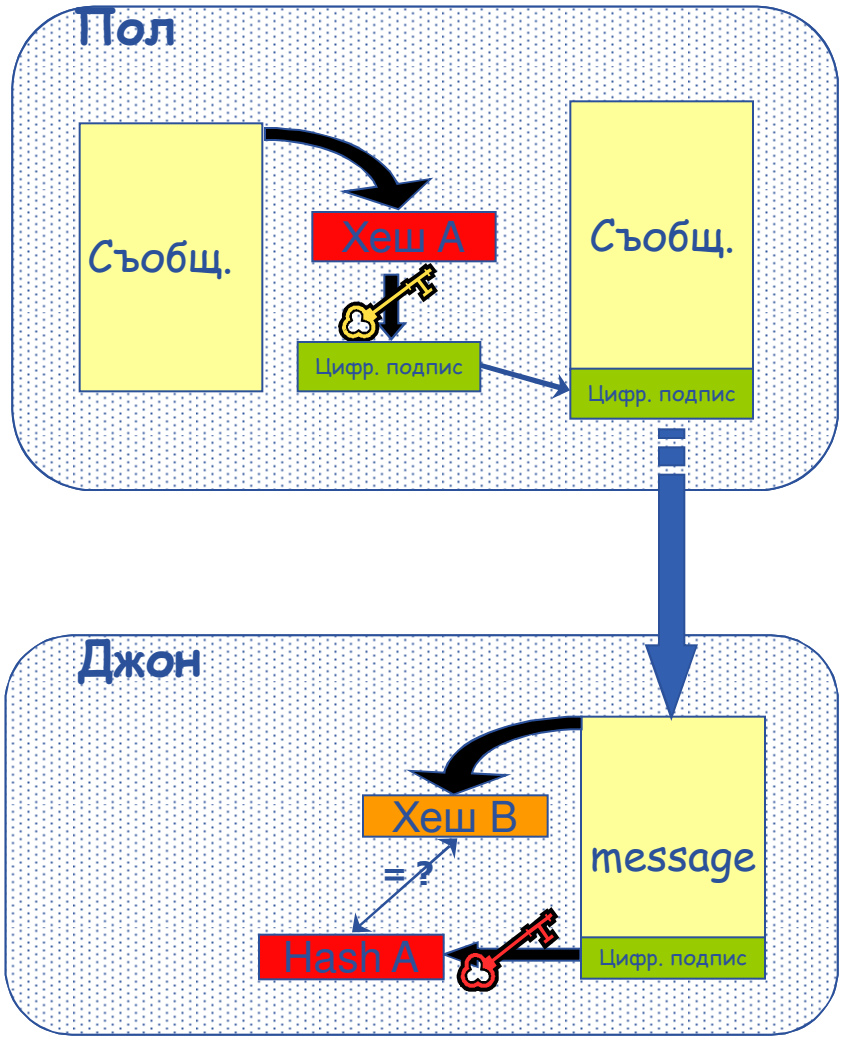
- **Всеки потребител има 2 ключа – частен и общодостъпен:**
  - *Невъзможно* е да се получи частния ключ от общодостъпния;
  - Съобщение, криптирано от единия ключ може да се декриптира **само** от другия.

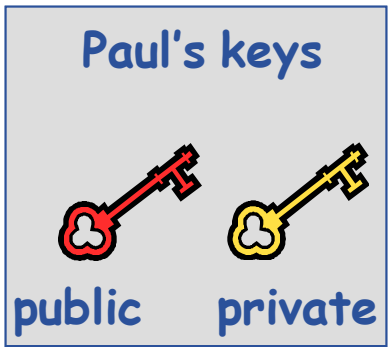

- **Концепция – опростена версия:**
  - Общодостъпните ключове се разменят
  - Изпращащият криптира с общодостъпния ключ на получателя
  - Получателят декриптира с частния ключ;



# Цифров подпис

- Пол **изчислява** *хеша* **на съобщението**
- Пол **криптира хеша със своя** *личен* **ключ: криптирания хеш е** *цифровия подпис*.
- Пол **изпраща подписаното съобщение на** Джон.
- Джон **изчислява хеша на съобщението**
- **Декриптира подписа, за да получи А, използва** *общодостъпния* **ключ на Пол.**
- **Ако хешовете са равни:**
  **1. съобщението не е модифицирано;**
  **2. хеш А е от частния ключ на Пол**



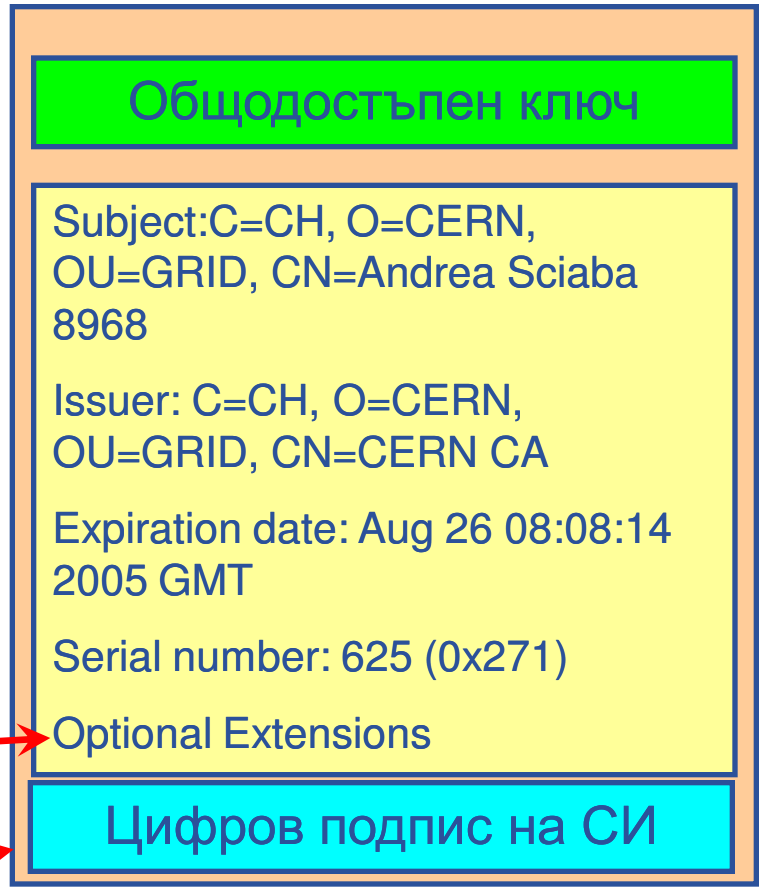
# Цифрови сертификати

- **Как може Джон да е сигурен, че общодостъпния ключ на Пол е в действителност на Пол, а не на някого другиго?**
  - Трета страна подписва сертификат, който свързва общодостъпния ключ и идентичността на Пол.
  - Както Джон, така и Пол се доверяват на тази трета страна

**“Сигурната трета страна” се нарича *Сертифициран Източник* (СИ).**

# X.509 Сертификати

- **X.509 сертификат съдържа:**
  - Общодост. ключ на притежателя;
  - Идентичност на притежателя;
  - Инф. за СИ;
  - Период на валидност;
  - Сериен номер;
  - Допълнителни разширения
  - Цифров подпис на СИ

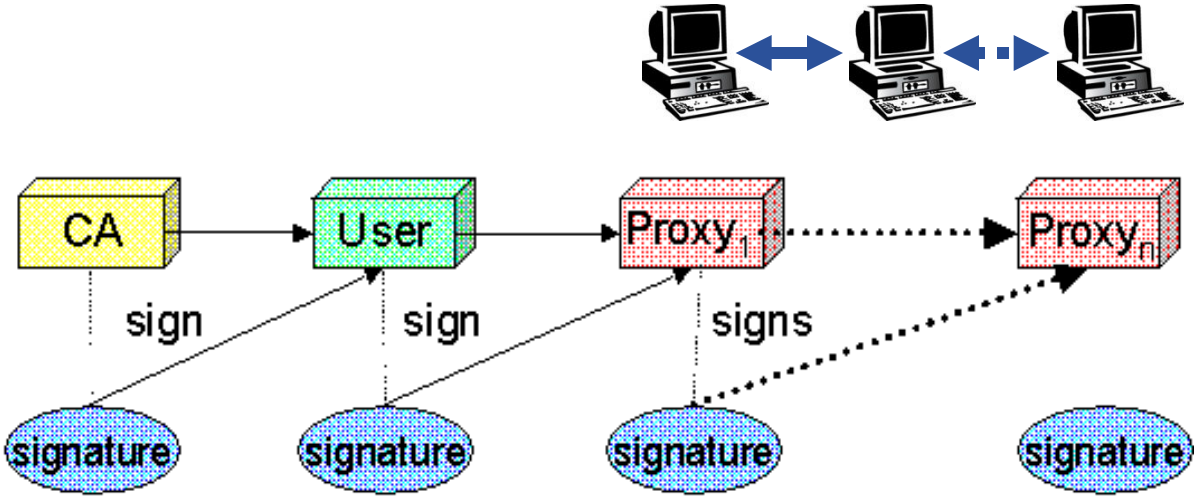


# Сертифициращи източници

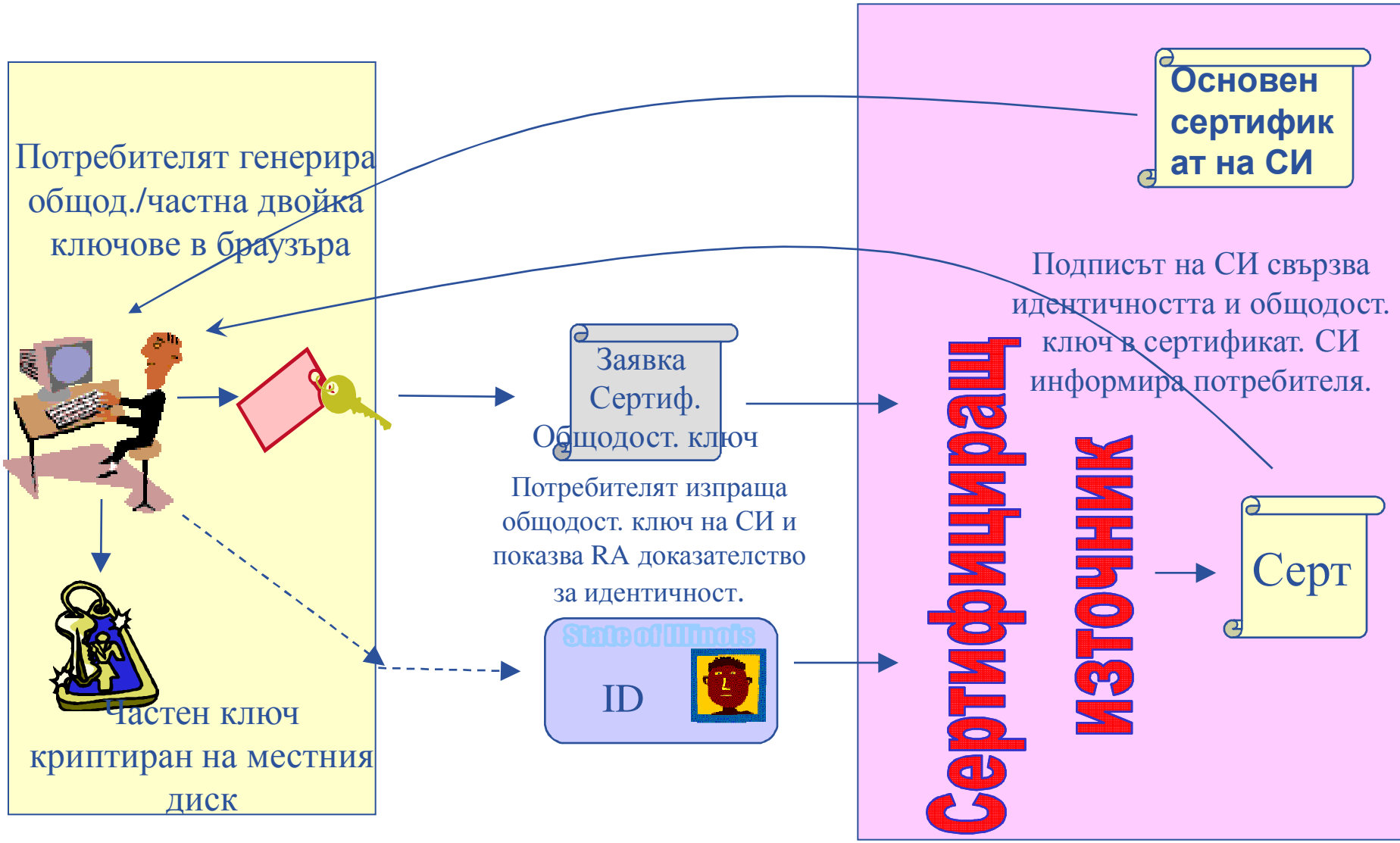
- Идентичността на потребителя може да се идентифицира от един от националните Сертифициращи Източници (СИ)
- Ресурсите също се сертифицират от СИ
- СИ се разпознават взаимно http://www.gridpma.org/,
- Всеки от СИ назначава определн брой хора, които са “регистриращи източници” РИ

# Сигурна Грид Инфраструктура - прокси

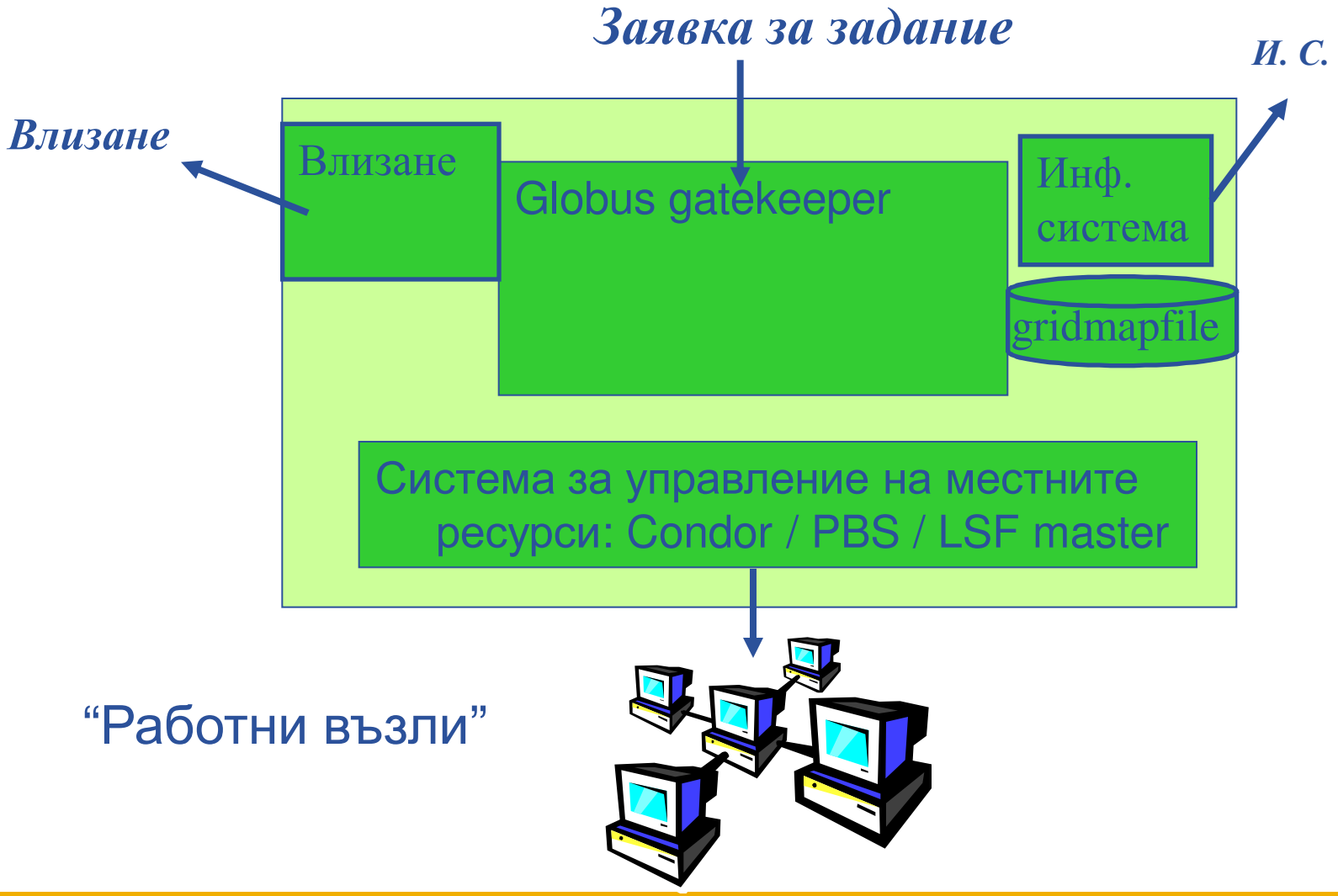
- **За подръжка на делегирането: А делегира на В правото да действа от името на А**
- **Прокси сертификати *разширяват X.509 сертификатите***
  - Краткосрочни сертификати подписани от потребителския сертификат или прокси
  - Намалява риска по сигурността, позволява делегиране



# Заявка за сертификат



# “Изчислителен елемент”: опашка за групови задания



# УЧВО: Услуга за членство във виртуалната организация

## Преди УЧВО (VOMS)

- **Потребителят се упълномощава като член на една ВО**
- **Всички членове на ВО имат същите права**
- **Gridmapfiles се обновяват от софтуера за управление на ВО: съпоставя потребителското DN към местния списък**
- **grid-proxy-init**

## УЧВО (VOMS)

- **Потребителят може да е в няколко ВО**
  - Общи права
- **ВО може да има групи**
  - Различни права за всеки
    - Различни групи от експериментатори
    - …
  - Групи в гнезда
- **ВО има роли**
  - Определена за дадена цел
    - Напр. системен админ.
    - Кога поема дадената длъжност
- **Прокси сертификата носи допълнителните атрибути**
- **voms-proxy-init**

# Отговорности на потребителя

- Да пази на сигурно място частния ключ – само на *USB памет*
- Да не заема сертификата на никого.
- Да докладва на своя локален/регионален отговорник, ако има проблеми със сертификата.
- Да не пуска делегираща услуга за по-дълго време, отколкото е необходимо за нуждите на настоящата задача.

**Ако вашия сертификат или делегирана услуга се използва от някой друг, не е възможно да се докаже, че това не сте вие.**

# Обобщение

- **Удостоверяване (Authentication)**
  - Потребителят получава сертификат от Сертифициращия Източник
  - Свързва се с UI чрез ssh
    UI е потребителския интерфейс към грида
  - Зарежда сертификата към UI
  - Единичен вход – към UI - създава прокси
  - След това **Инфраструктурата на грид по сигурността използва прокси**

- **Упълномощаване (Authorisation)**
  - Потребителят се присъединява към Виртуална организация (Virtual Organisation)
  - VO осигурява достъпа до Грид ресурсите
  - Gridmapfile (или подобни) прави съответствието на потребителя към местния списък