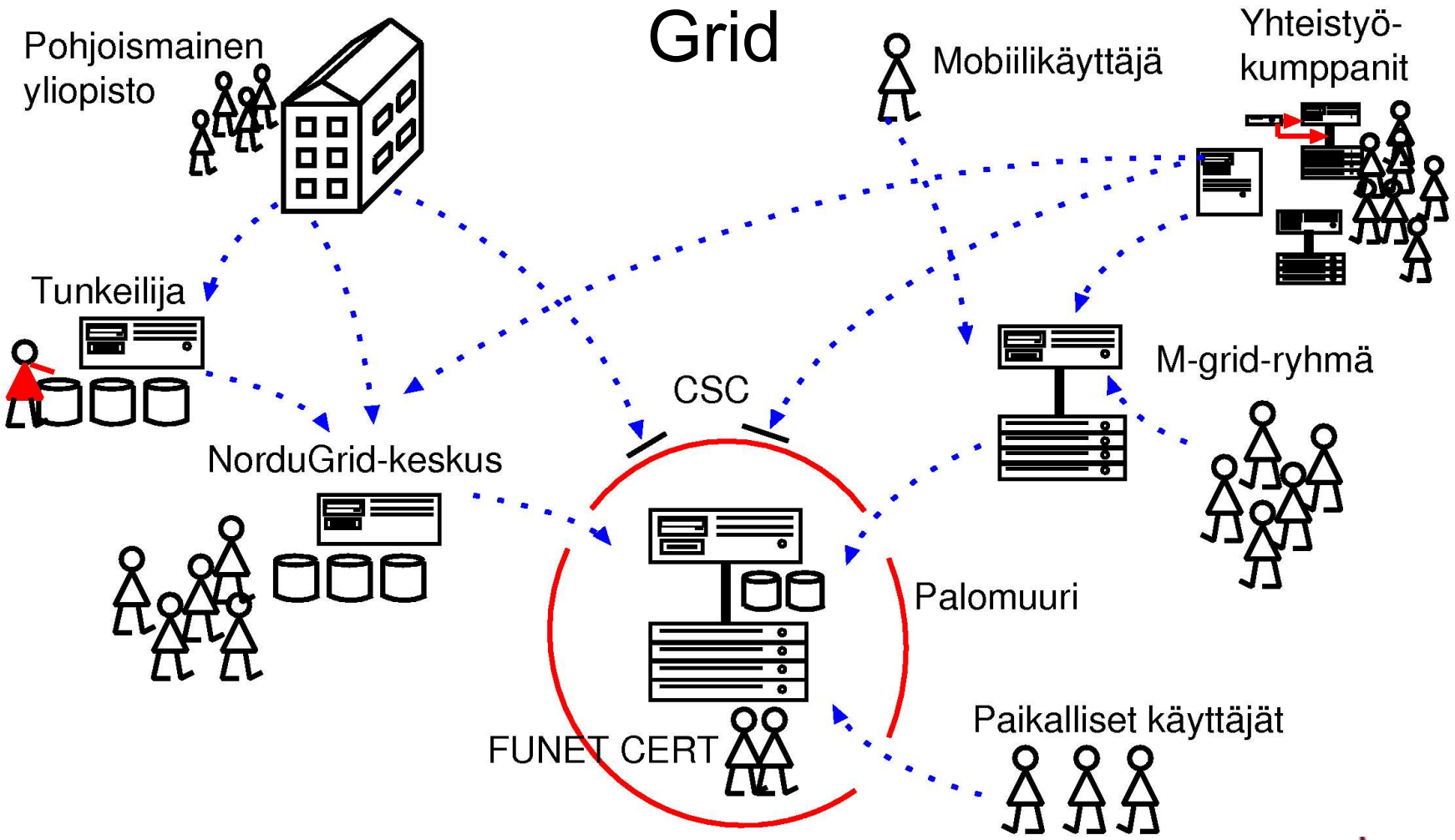
# Tietoturvan haasteet grideille

Arto Teräs <arto.teras@csc.fi>

Suomen Unix-käyttäjäin yhdistys FUUG ry:n kevätristeily

20.3.2006


Grid
Pohjoismainen yliopisto
Mobiilikäyttäjä
Yhteistyö-kumppanit
Tunkeilija
M-grid-ryhmä
CSC
NorduGrid-keskus
Palomuuri
FUNET CERT
Paikalliset käyttäjät

# Tavoite

- **Helppo pääsy suureen joukkoon erilaisia resursseja**
- **Suuri laskenta- ja tallennuskapasiteetti**
- **Käyttö mistä vain, milloin vain (mobiilikäyttäjät)**
- **Ei käyttöä haittaavia rajoitteita siinä mitä saa tehdä (esim. omien ohjelmien suorittaminen)**
- **Yksityisyyden suoja turvattu**

**Mutta:**

- **Halu estää väärinkäyttö**
- **Resurssien jako, käytäntöjen yhteensovittaminen yli organisaatiorajojen**

# Avoimuuden kulttuuri

- **Nykyisissä grid-hankkeissa yhtäläisyyksiä Internetin alkuaikoihin**
  - Yritetään nyt ensin saada edes yhteydet toimimaan, mietitään tarkempia rajoituksia myöhemmin
  - Jotain opittu: ei selväkielisiä salasanoja verkon yli. Mutta miten hallita käyttöoikeuksia?
- **Aloite grid-ympäristöjen rakentamiseen soveltavien tieteiden piiristä, ei tietojenkäsittelytieteilijöiltä**
  - Ensimmäisiä käyttäjiä fyysikot, joiden data ei ole arkaluontoista
  - Toisaalta hyvissä ajoin liikkeellä myös lääketieteen ala, jolla tiukat turvavaatimukset

# Käyttäjän tunnistus

- **Julkisen avaimen salausmenetelmistä vahva perusta**
- **Kaksi yleisesti käytettyä mallia:**

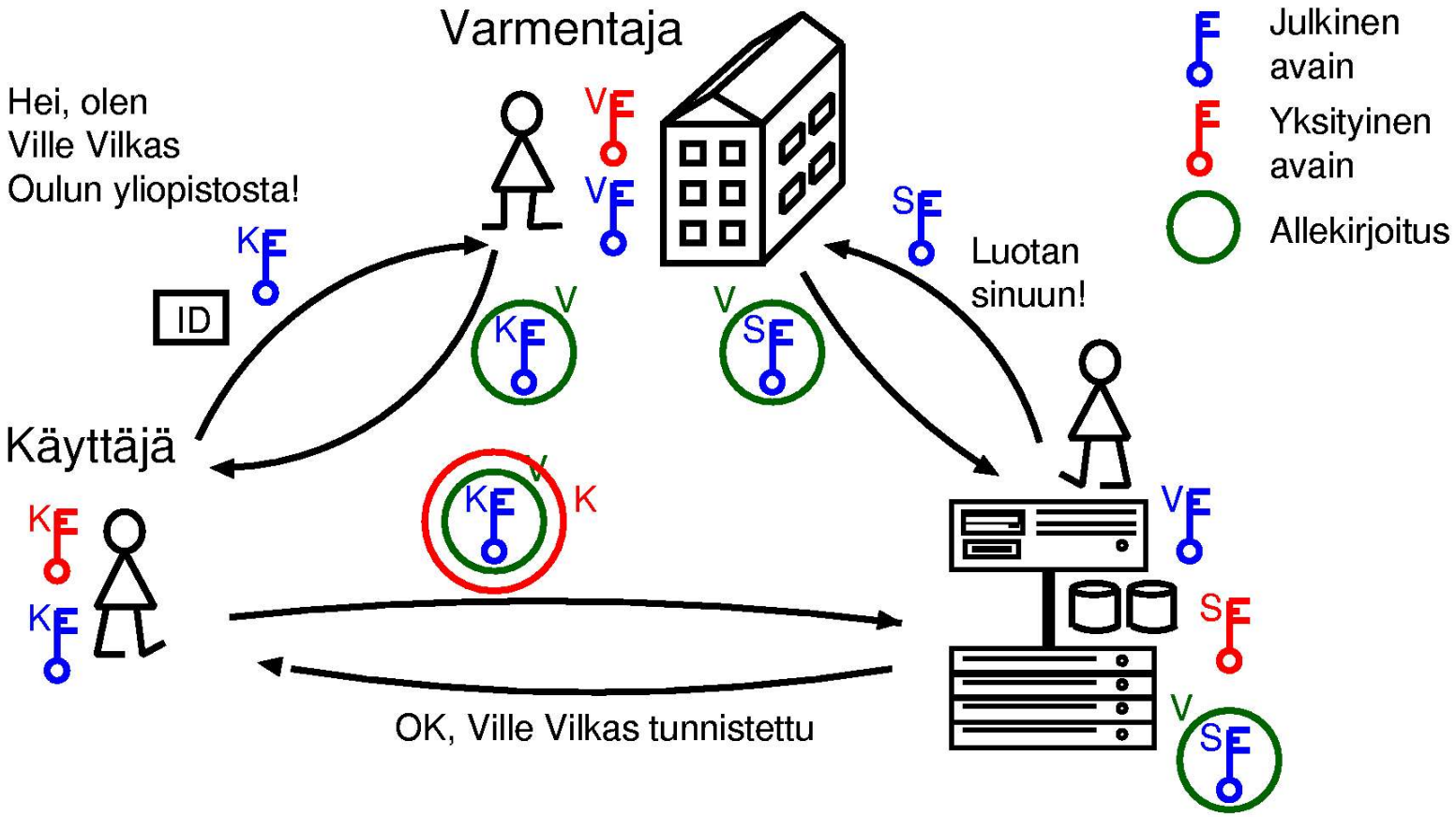
  1) Henkilövarmenteet (luotettu kolmas osapuoli)

  2) Tunnistuksen siirtäminen kotiorganisaatioon ja suojattu yhteys palvelimien välillä (Shibboleth)

  \+ näiden kytkeminen toisiinsa (GridShib)

- **Haasteita:**
  - Identiteetin kaappauksen estäminen
  - Tunnistautuminen epäsuorasti - miten ohjelma voi esiintyä gridissä käyttäjän identiteetillä?
- **Yksityisyyden suoja, anonyymi käyttö?**

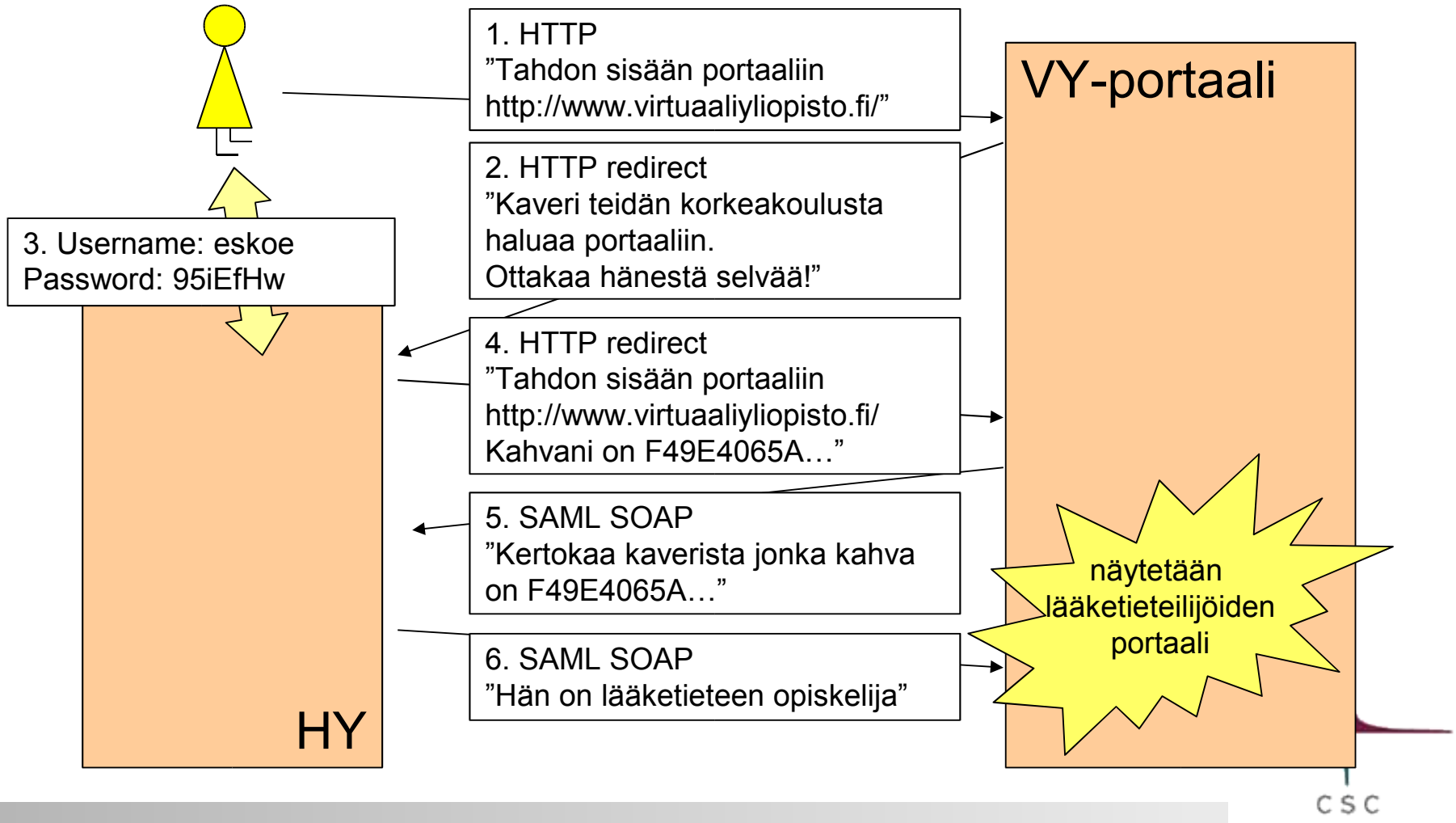
# Varmenteisiin perustuva tunnistus



# Varmenteisiin perustuva tunnistus

- **Mihin tallennetaan käyttäjän yksityinen avain?**
  - Tiedostoon omalla koneella? Suojattuna?
  - Erilliselle turvatulle palvelimelle?
  - Toimikortille? Matkapuhelimen SIM-kortille?
- **Keihin varmentajiin pitäisi luottaa?**
  - Akateemisia ja kaupallisia varmentajia
  - Varmentajien muodostamat luottamusverkostot (esim. EUGridPMA, International Grid Trust Federation) ovat ratkaisseet tämän ongelman jo melko hyvin

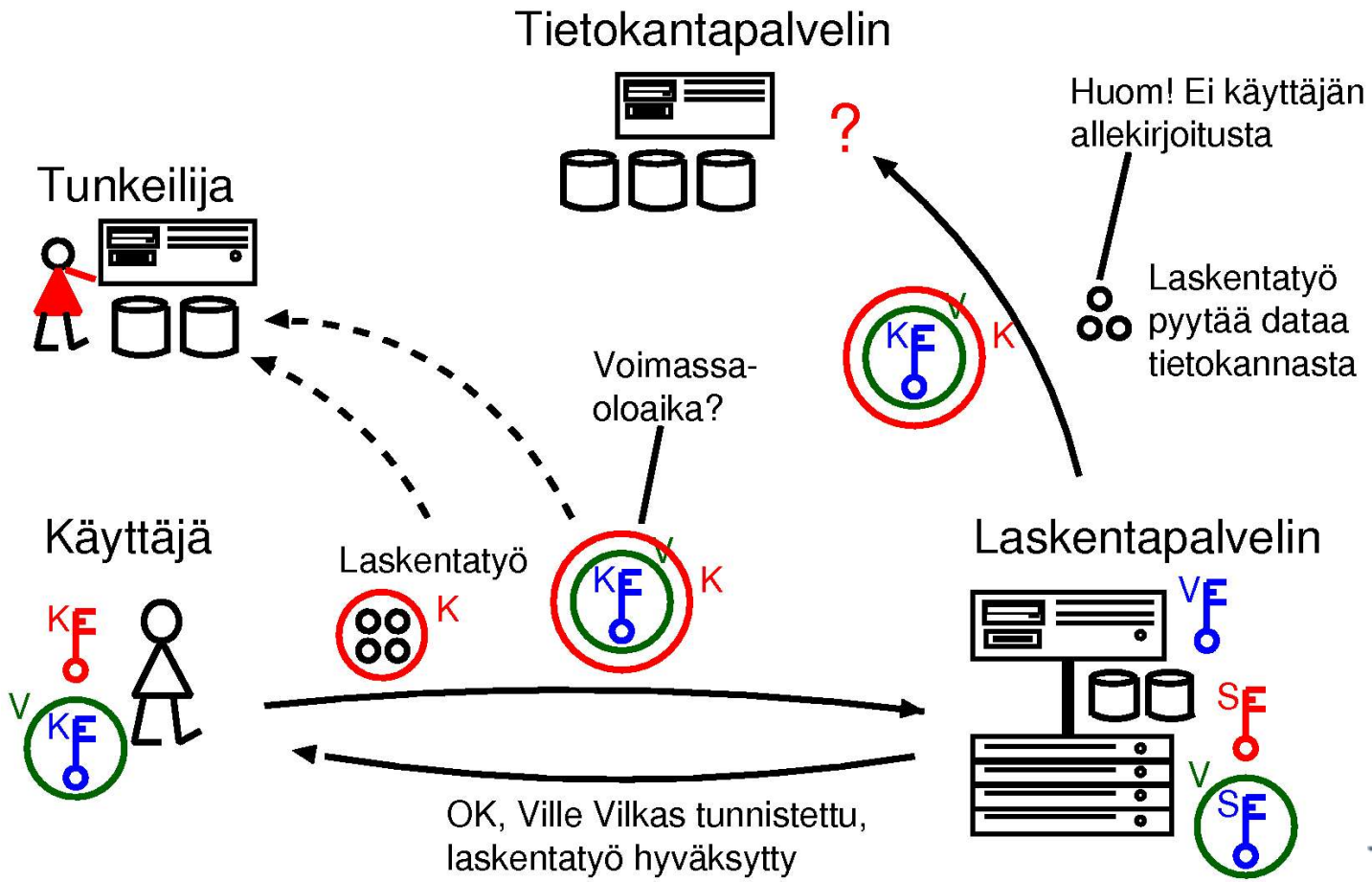
# Tunnistuksen siirto "kotiin" (Shibboleth)



# Käyttöoikeuksien hallinta

- **Erotettu käyttäjän tunnistuksesta**
  - Palvelu voi tunnistaa käyttäjän, mutta silti evätä pääsyn (vrt. perinteinen unix-tunnus ja salasana, jossa nämä yhdistetty)
- **Käyttäjiä hallitaan tyypillisesti ryhminä (Virtual Organization, VO)**
  - Hallinta yksittäisten käyttäjien tasolla olisi liian työlästä
- **Luottamus VO:ta ylläpitävään organisaatioon!**
- **Hienojakoisuuden ja joustavuuden ristiriita**
  - Nykyisin yleisesti käytössä karkea malli jossa yksi “pääsylippu” kaikkeen
  - Kehittyneemmät mallit: roolit, ja erillinen tunniste kutakin operaatiota varten, mutta käyttäjälle silti kertakirjautuminen

# Oikeuksien siirto (delegation)



# Palomuurit

- **Kiinteät ip-osoitteisiin ja portteihin perustuvat säännöt soveltuvat huonosti grid-ympäristöihin**
  - Haittaavat käyttäjien liikkuvuutta
  - Laajat yhteistyöverkostot:: pääsy pitäisi joka tapauksessa sallia suuresta joukosta eri verkkoja => hallinta vaikeaa
- **Estävät lähinnä sokeat automatisoidut hyökkäykset satunnaisista osoitteista**
  - Hyöty pienenee sitä mukaa mitä enemmän on luvallisia käyttäjiä ja sallittuja verkkoja
- **Kaapattu tunnus on todennäköisempi tunkeutumisväylä kuin ohjelmiston tietoturva-aukko**

# Tietoturvapoikkeamat

- **Tunkeutumistavat eivät juurikaan eroa nykyisistä**
- **Havaitsemisessa paras tulos saataneen yhdistämällä vanhat keinot ja muutamia uusia**
  - Grid-tason IDS?
- **Reagoinnin nopeus korostuu**
  - Kaapatulla tunnuksella päästään entistä nopeammin etenemään laajalle alueelle
- **Yhteistyö organisaatiorajojen yli**
  - CERTit tehneet jo pitkään, varmaankin tältä osin kaikkein parhaiten grideihin valmistautunut yhteistyöverkosto
  - Toiminta varmenneviranomaisten (CA) kanssa, kaapattujen tunnusten varmenteiden mitätöinti pääsyn sulkemiseksi

# Käyttöpolitiikka ja säännöt

- **Käyttäjä ei jaksa lukea pitkiä ohjeita ja sääntöjä — ei ainakaan useita erilaisia!**
  - Sääntöjen yhtenäistäminen eri organisaatioiden välillä tärkeää
- **Käyttöoikeuden saaminen eri palveluihin pitää olla helpompaa kuin nykyisten käyttäjätunnusten**
  - Miten käyttäjähallinnot saadaan pelaamaan yhteen?
- **Käyttäjän pelottelu ja tekniset rajoitukset vai käyttäjään luottaminen?**
- **Miten käyttäjä saadaan luottamaan gridiin — sääntöjä palveluntarjoajille?**
- **Kansainvälinen yhteistyö ja kulttuurierot**

# Linkkejä

- **Haka-infrastruktuuri:**
  **http://www.csc.fi/suomi/funet/middleware/haka/**
- **Shibboleth-väliohjelmisto:**
  **http://shibboleth.internet2.edu/**
- **Globus Security Infrastructure:**
  **http://www.globus.org/toolkit/docs/4.0/security/**
- **EGEE Security work package:**
  **http://egee-jra3.web.cern.ch/egee-jra3/**
- **Grid Security Papers:**
  **http://www.princeton.edu/~jdwoskin/grid/gridsecpapers.html**