Token HW

- Da completare le prove per Aladdin
- Inizio sperimentazione: Febbraio 2008
  - 50 /100 utenti per 6 mesi?
  - certificati personali e robot
  - da modificare il CP/CPS dell'INFN CA
    - studiare progedura di gestione non troppo pesante

Servizi essenziali: DNS

- DNS
  - Template (con bind-chroot e servizi accessori necessari) + script di configurazione lato utente finale (zone => named.conf) pronti.
  - Sarebbe opportuno definire un'architettura base di virtualizzazione standard (anche per il log-server e le auditing box locali): nuovo sottogruppo di HA?
  - Una volta definita tale architettura in ~2 mesi si potrebbe arrivare alla versione finale di produzione (cioe' distribuibile).

Servizi essenziali: log server

- syslog-ng & OSSEC
  - log analysis
    - esempi:
      - Rule: 11 fired (level 8) -> "Excessive number of events (above normal)."
        Portion of the log(s):
        The average number of logs between 3:00 and 4:00 is 16947. We reached 22033.
      - Rule: 5712 fired (level 10) -> "SSHD brute force trying to get access to the system."
        Portion of the log(s):
        Dec 9 21:20:06 ficcanaso sshd[51693]: Invalid user 123456 from 81.22.101.142
      - Rule: 5104 fired (level 8) -> "Interface entered in promiscuous (sniffing) mode."
        Portion of the log(s):
        Dec 7 13:25:13 localhost kernel: device eth0 entered promiscuous mode
  - system integrity analysis (server – agent)
      - Rule: 552 fired (level 7) -> "Integrity checksum changed again (3rd time)."
        Portion of the log(s):
        Integrity checksum changed for: '/home/www/htdocs/stats/index.html'
  - rootkit checker (server - agent)
  - active response: NO