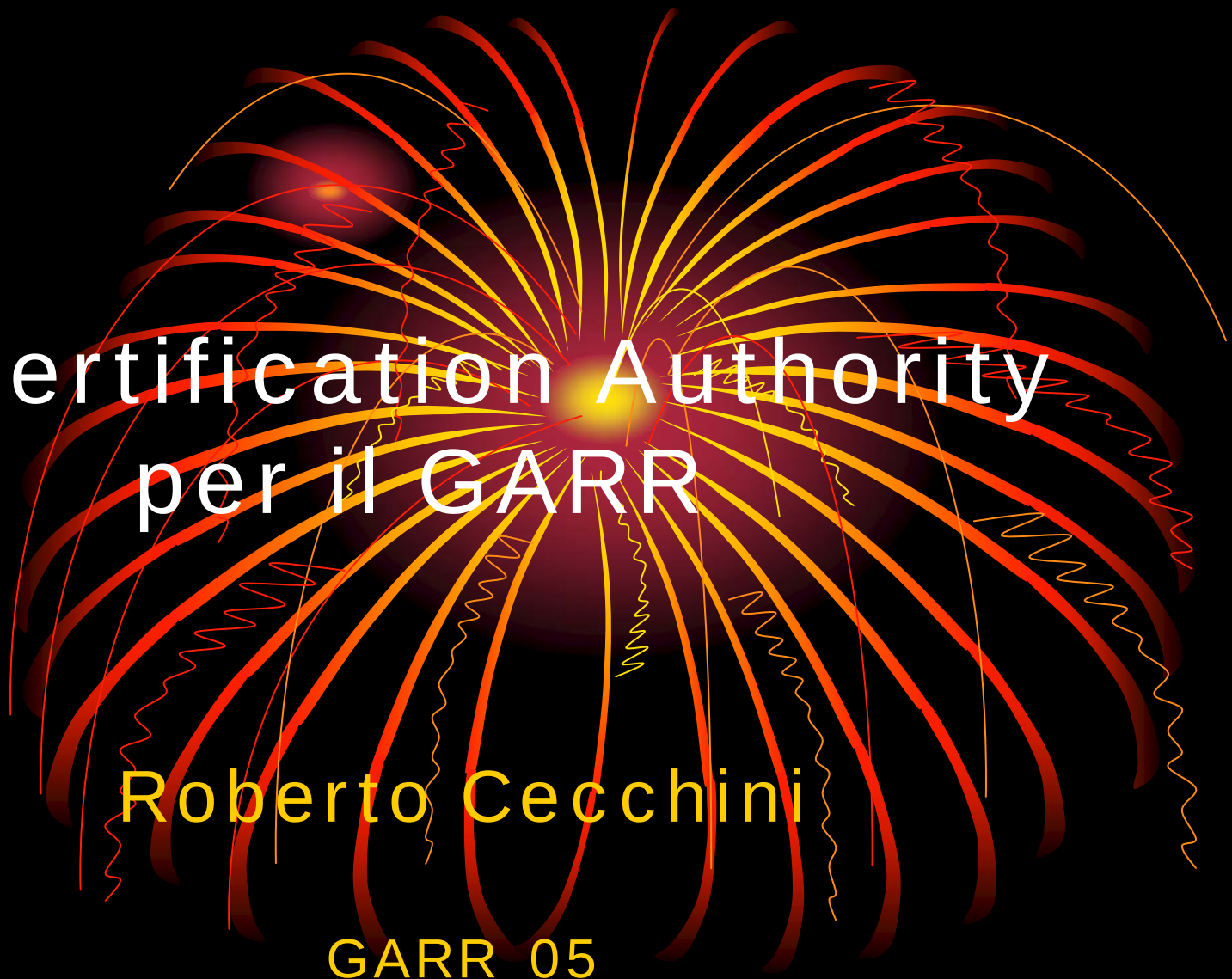


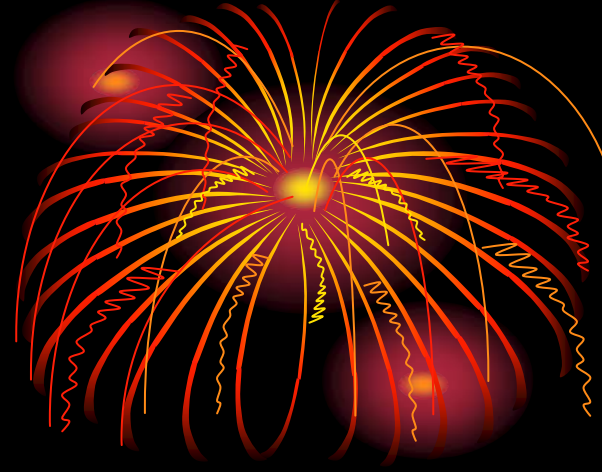
La Certification Authority per il GARR

Roberto Cecchini

GARR_05

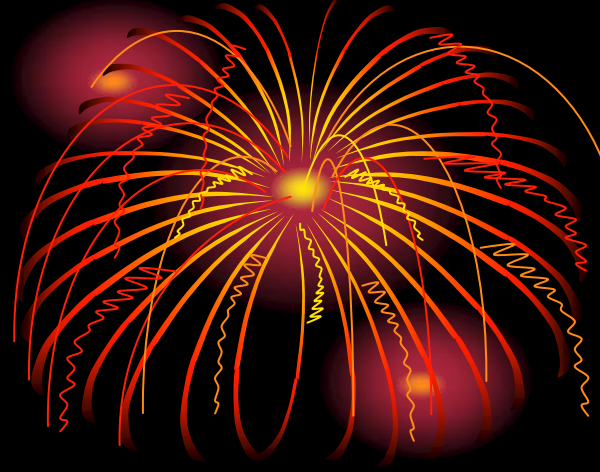
Pisa, 12 Maggio 2005

Perché X.509?



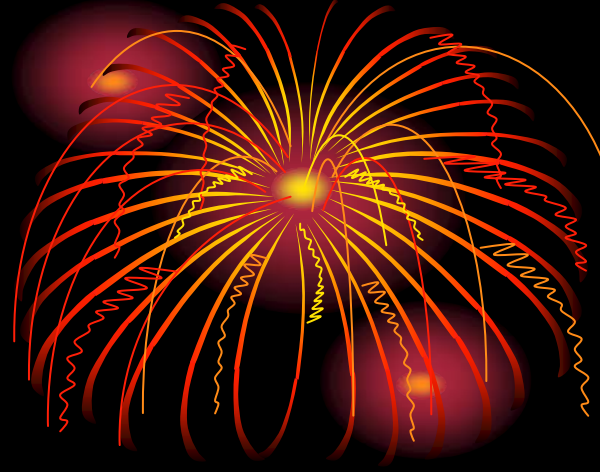
- PGP
  - uso più “locale”, all’interno di una comunità abbastanza ben definita
- X.509
  - più indicato ad un ambiente eterogeneo quale la comunità GARR
  - autenticazione utenti e server
  - “griglie di calcolo”: numerosi progetti internazionali (ad es. LCG, EGEE) e italiani
  - infrastruttura di Autenticazione e Autorizzazione (AAI)
    - EduRoam, GN2

Perché GARR CA?



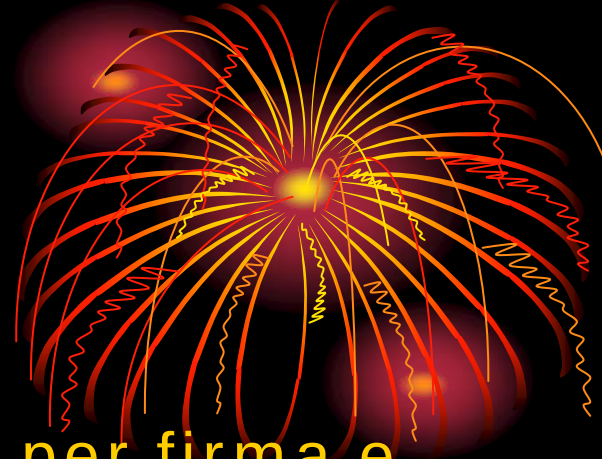
- L'istituzione di una CA è un'operazione abbastanza delicata, non tanto per la parte software, quanto per quella gestionale.
- Opportuno che il GARR si faccia carico anche di questo servizio, come hanno già fatto molte altre NREN europee:
  - Olanda, Svizzera, Germania, Spagna, Portogallo, Finlandia...

Caratteristiche

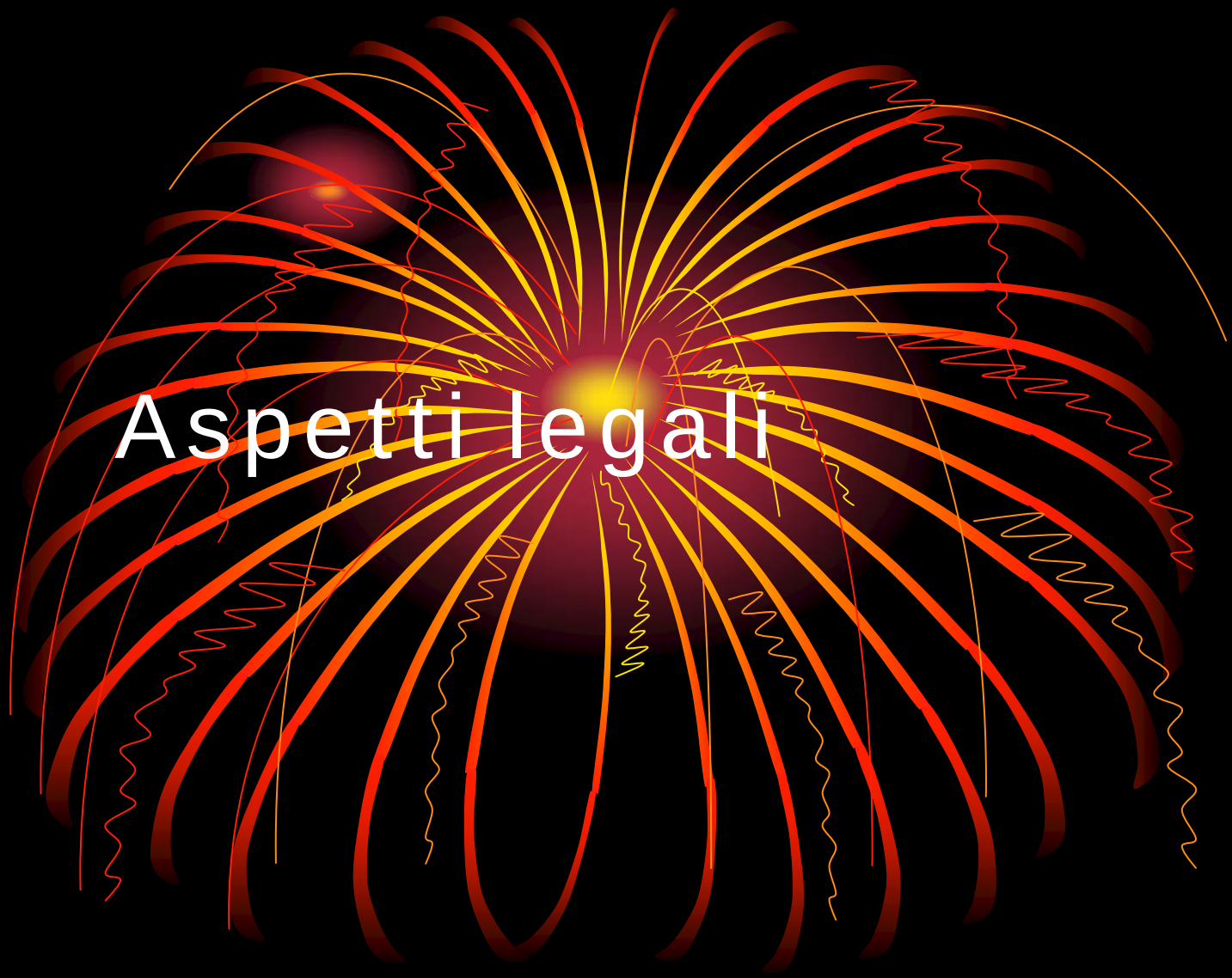


- Una CA per tutto il GARR:
  - istituzioni locali per autenticazione utenti e verifica richieste (Registration Authority: RA).
  - da valutare la possibilità di CA di "secondo livello", ad esempio come in Francia e in Svizzera.
- Si interfaccerà con le altre CA europee per realizzare i meccanismi di AA, indispensabili per gli utenti roaming.

Servizi



- Rilascio di certificati personali per firma e cifratura di messaggi e file (anche su *smart card*?)
- rilascio di certificati per server e servizi;
- emissione di CRL;
- servizio OCSP;
- repository online http e LDAP (7/24):
  - richiesta e consultazione certificati;
  - documentazione;
  - CRL.



Aspetti legali

DPR 445/2000, Art. 10

- Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio è liberamente valutabile, in relazione alle sue caratteristiche oggettive di qualità e sicurezza
- Quando è sottoscritto con firma digitale, o con altra firma elettronica avanzata e la firma è basata su di un certificato qualificato e generata con un dispositivo per la firma sicura, fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

DPR 445/2000, 29-quinquies

- Sottoscrizione di documenti informatici
  - di rilevanza esterna
    - le pubbliche amministrazioni possono svolgere direttamente attività di rilascio dei certificati qualificati o possono rivolgersi a certificatori accreditati
  - di rilevanza interna
    - ciascuna amministrazione può adottare regole diverse da quelle contenute nelle regole tecniche (DPCM 13/01/2004)