# Certificati e mTLS OCP

## Punti da analizzare

* ! Definire Perimetro REQUIRED per le Prossime MILESTONE:
  + Utilizzo mTLS solo all’interno del cluster o anche per chiamate provenienti dall’esterno
  + Utilizzo certificati self-signed creati da Istio o utilizzo di certificati custom CA
  + Modalità strict o permissive
* ! Gestione doppio FQDN nei certificati utilizzati per garantire ai servizi di BE nel cluster di **poter essere abilitati a rispondere sia ai cluster.local (interni) che ai \*.cariprc.it (esterni)**
  + **OWNER: Red Hat per approfondimento tecnico su Soluzione;**
  + **VALIDAZIONE: Sicurezza**
* ! **Accertare che la comunicazione tra il Proxy Istio e la terminazione del micro-gateway sia garantita in https. In caso contrario avremmo problema sul micro-gateway nelle chiamate entranti.**
  + **OWNER: Red Hat per proposta soluzione in linea con la richiesta,**
  + **VALIDAZIONE: NTT e Sicurezza**
* ! **Soluzione per gestione traffico in uscita tramite EgressIP :**
  + **OWNER: Red Hat e Bagiotti, per la scelta della soluzione migliore secondo esigenze espresse;**
  + **SUPPORTO: NTT;**
  + **VALIDAZIONE: SICUREZZA**
* ! **Gestione del ciclo di vita e del processo di change delle Istio Auth Policy (RFC, chi le apre, chi le esegue e come)**
  + **OWNER: Imola;**
  + **SUPPORTO: NTT, Red Hat, Infra CAGS**
* **Gestione e ciclo di vita dei certificati, con due macro-attività distinte:**
  + **(priorità da definire) Disegno/documentazione a Red Hat che mostri in modo chiaro il ciclo di vita di un certificato e le interazioni con le varie automazioni e la soluzione suggerita in base all’esperienza sui propri clienti**
    - **OWNER: Red Hat come descrizione E2E della soluzione di gestione certificati;**
    - **VALIDAZIONE: Sicurezza, NTT**
  + **(priorità da definire) Definizione soluzione CAGS per gestione e manutenzione del ciclo di vita dei certificati** 
    - **OWNER: INFRA CAGS (Bagiotti, Guglielmo)**
    - **Supporto: Red Hat, NTT**
    - **Validazione: Sicurezza**