UNIVERSITÀ DEGLI STUDI
DI MILANO

DESIGN AND DEVELOPMENT OF AN ASSURANCE METHODOLOGY FOR SECURITY CERTIFICATIONS IN HIGHLY DYNAMIC ARCHITECTURES

Relatore: ***Prof. Claudio A. Ardagna***
Co-Relatore: ***Dr Nicola Bena***

Contesto (1)

Web service tradizionali

- Statici e monolitici
- I fornitori dei servizi web erano costretti a gestire l'intera infrastruttura

Cloud

- Dinamico e flessibile
- I fornitori dei servizi web devono solo pensare al software del proprio servizio
- Servizio migliore e rapido per gli utenti

Contesto (2)

Edge

- Migliora il concetto di decentralizzazione
- Introduce i nodi computazionali distribuiti per basse latenze
- Permette ai sistemi IoT di svilupparsi ulteriormente

IoT

- Numerosi dispositivi coinvolti
- In continuo cambiamento
- Il cambiamento di un dispositivo non deve bloccare il sistema

Certificazione

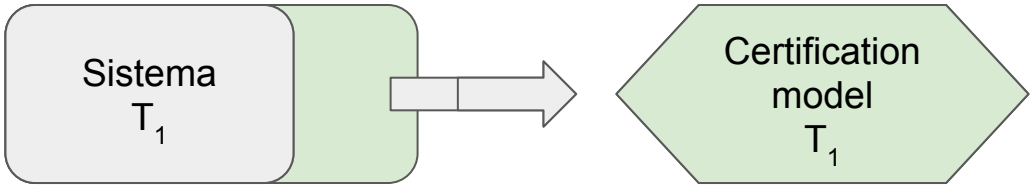
I sistemi informatici garantiscono la propria sicurezza usando un sistema di certificazioni.

- Lunga e costosa analisi del sistema
- Rilasciano un certificato che attesta la presenza di determinate proprietà
- Non contemplano cambiamenti nella configurazione del sistema

Obiettivi

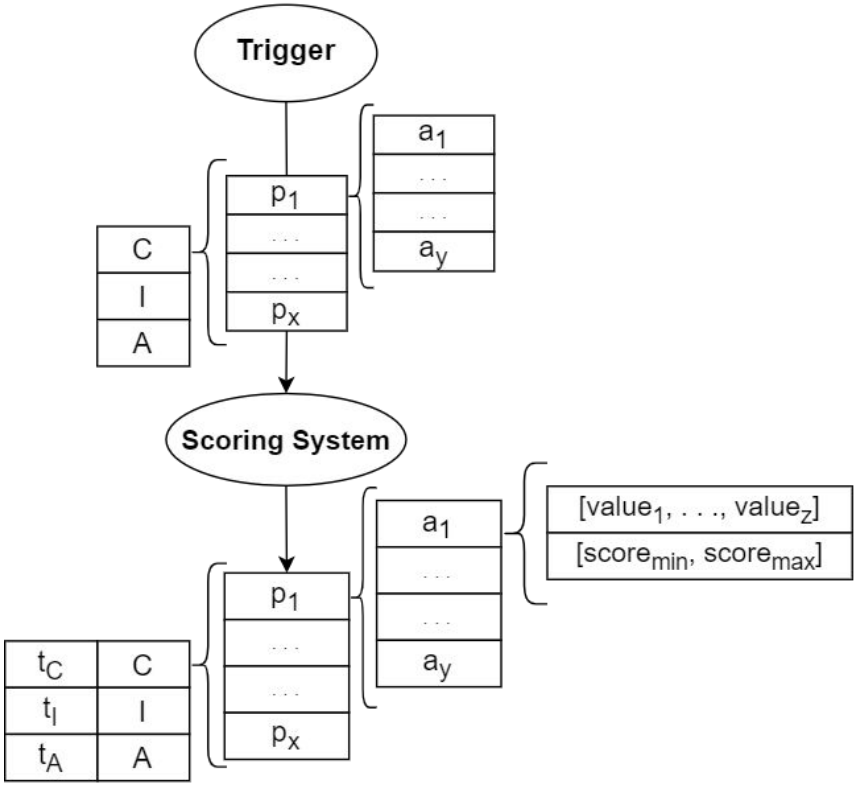
Fornire un primo approccio al problema proponendo un nuovo schema di certificazione

- Permette piccoli cambiamenti alla configurazione
- Analisi dei soli aspetti modificati
- Rapido, leggero e meno ridondante
  - Il modello deve evolversi assieme al sistema



Schema di Certificazione Effimera (1)

- **Proprietà e attributi**
  - a = attributo
  - p = micro-proprietà
  - t = soglia
  - C = Confidenzialità
  - I = Integrità
  - A = Disponibilità
- Trigger
- Scoring system



Schema di Certificazione Effimera (2)

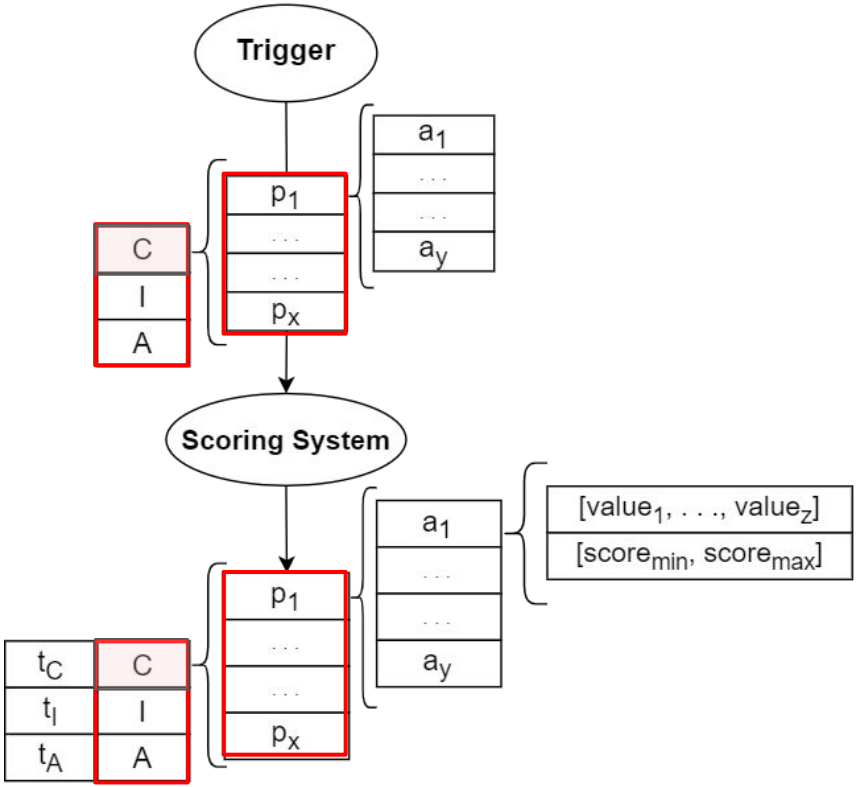
Proprietà e attributi

Micro-proprietà: Specifico criterio usato per valutare l'operato del sistema.

Esempio

Encryption/Decryption

Abilità di un sistema di eseguire correttamente algoritmi di criptazione per cifrare e decifrare messaggi



Schema di Certificazione Effimera (3)

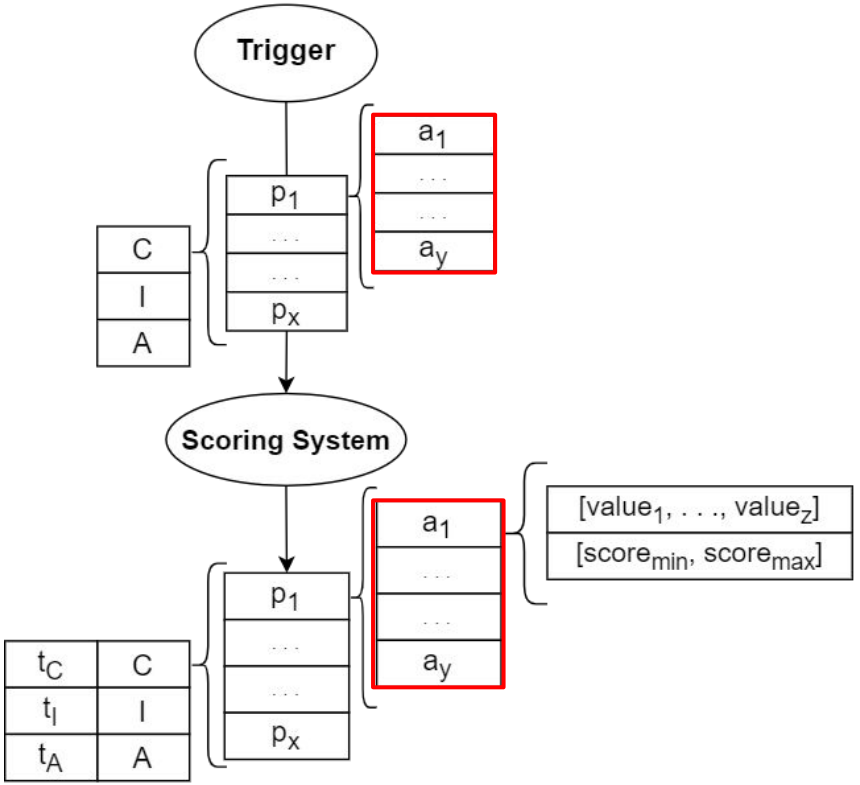
Proprietà e attributi

Attributi: Componenti delle micro-proprietà

Esempio

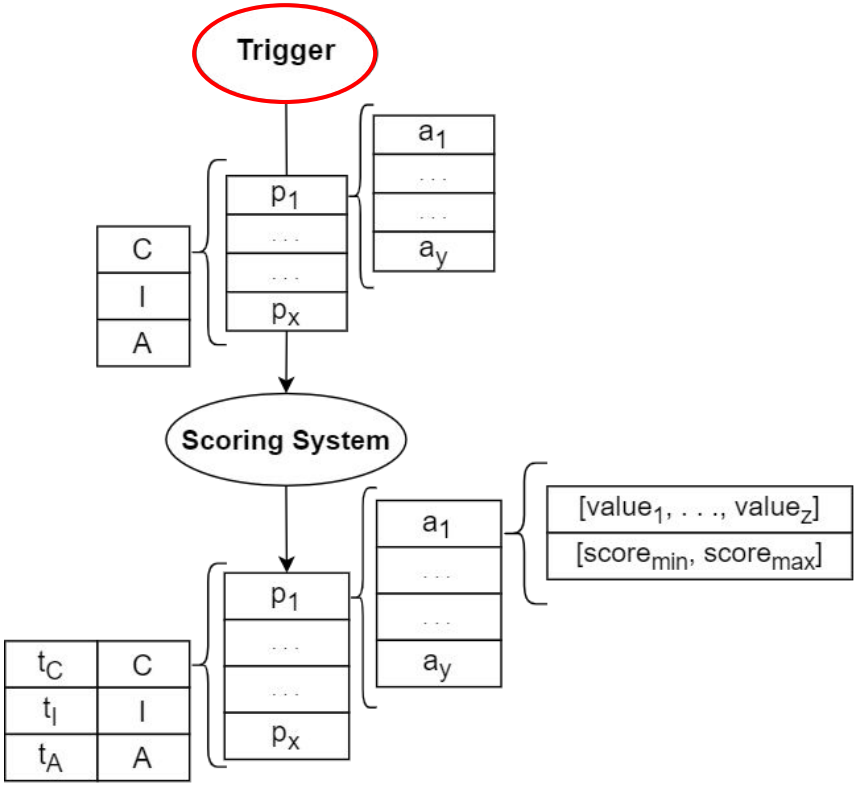
Encryption/Decryption

Lunghezza chiave AES-GCM ⇒ 256 bit



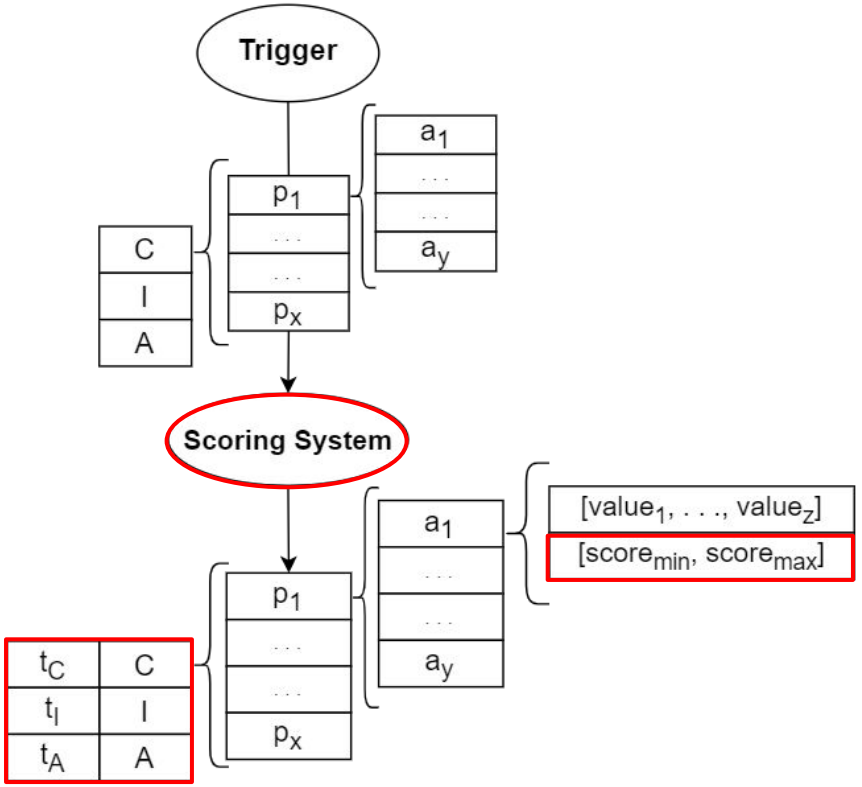
Schema di Certificazione Effimera (4)

- Proprietà e attributi
- **Trigger**
  - Monitoring
  - Valutazione cambiamenti
  - Avviamento del processo
- Scoring system



Schema di Certificazione Effimera (5)

- Proprietà e attributi
- Trigger
- **Scoring system**
  - Assegnato da un esperto
  - Tasso di proprietà
  - Standard
  - Soglia



Schema di Certificazione Effimera (7)

$$Ephemeral(\mathcal{C}, system_{t+1}) \rightarrow \mathcal{M}_{t+1}$$

- $\mathcal{C} \rightarrow$ Insieme dei certificati precedentemente ottenuti
- $system_{t+1} \rightarrow$ Sistema dopo l'update
- $\mathcal{M}_{t+1} \rightarrow$ Certification model per il sistema aggiornato

Schema di Certificazione Effimera (8)

$$Execute(\mathcal{M}_{t+1}) \rightarrow \mathcal{C} \cup \{c_{t+1}\}$$

- $\mathcal{C} \rightarrow$ Insieme dei certificati precedentemente ottenuti
- $c_{t+1} \rightarrow$ Nuovo certificato parziale
- $\mathcal{M}_{t+1} \rightarrow$ Certification model per il sistema aggiornato

Esempio di Esecuzione (1)

1) Prima certificazione

2) Software update

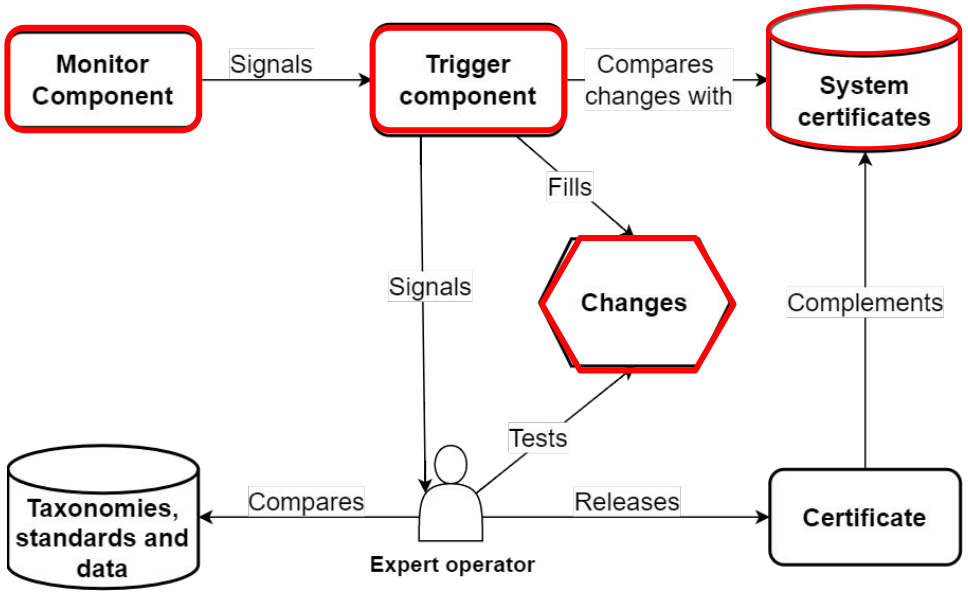
3) Ricertificazione

Requirement
Cryptographic Key Generation
Cryptographic Key Destruction
Cryptographic Operation - Encryption/Decryption
Cryptographic Operation - Hashing
Cryptographic Operation - Signing
Cryptographic Operation - Keyed-Hash Message Authentication
Random Bit Generation
TLS Protocol

$$\{(p_1, \{e_1\}), (p_2, \{e_2, e_3\}), (p_3, \{e_4, \ldots, e_9\}), (p_4, \{e_{10}, \ldots, e_{15}\}), (p_5, \{e_{16}\}),$$
$$(p_6, \{e_{17}\}), (p_7, \{e_{18}, \ldots, e_{28}\}), (p_8, \{e_{29}\})\}$$

Esempio di Esecuzione (2)

- **Encryption/Decryption**
  - Condizioni AES-GCM
  - Algoritmo e lunghezza della chiave
- **Signing**
  - Algoritmo e lunghezza della chiave
- **TLS Protocol**
  - Condizioni DTLS Handshake



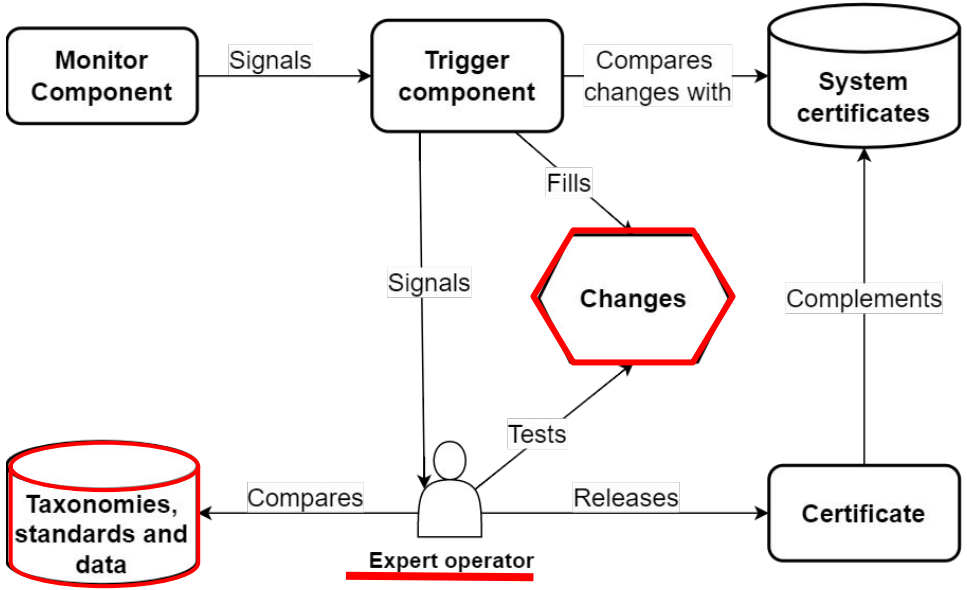
Esempio di Esecuzione (3)

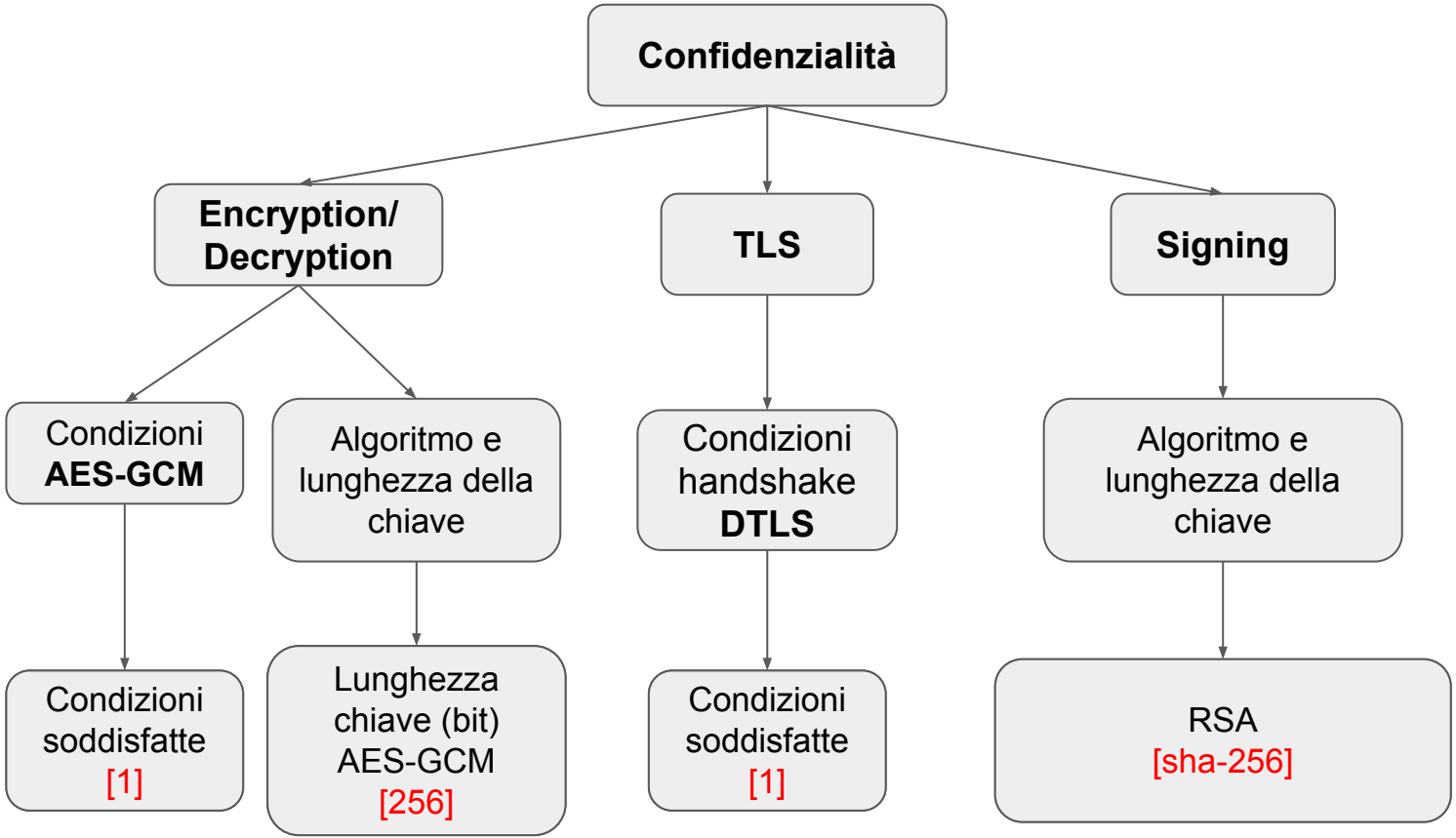
Compiti operatore

1) Assegna una lista di valori possibili ad ogni attributo

2) Assegna un range di score ad ogni attributo

3) Assegna una soglia ad ogni macro-proprietà coinvolta





Macro-Proprietà

Micro-Proprietà

Attributi

Valori

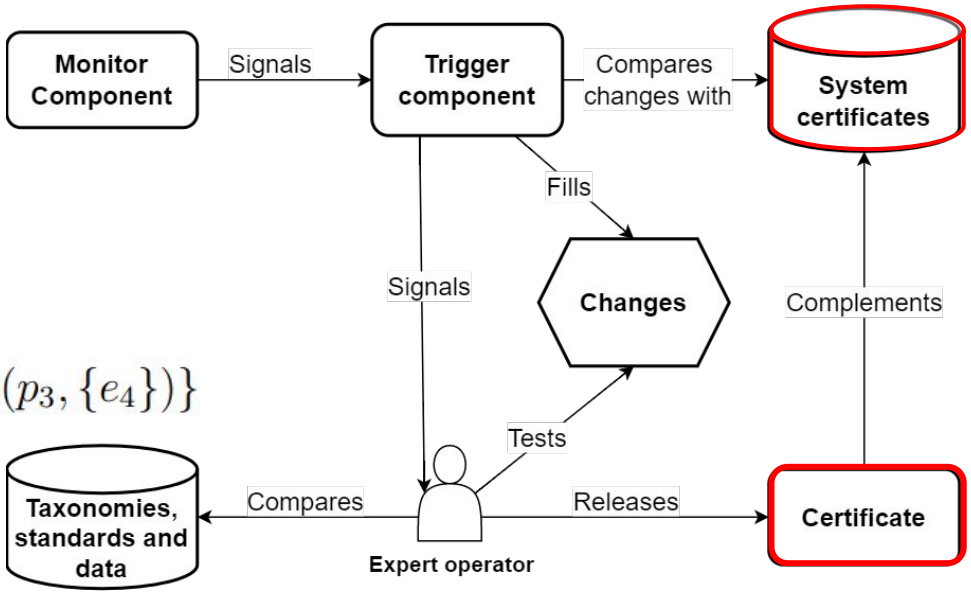
Esempio di Esecuzione (4)

Rilascio del certificato

$$\mathcal{E} = \{\{t_1, t_2\}_{p_1}, \{t_3\}_{p_2}, \{t_4\}_{p_3}\}_{Confidentiality}$$

$$\mathcal{M} = \langle P_1, \mathcal{E} \rangle$$

$$Execute(\mathcal{M}) \rightarrow \mathcal{C} \cup \{(p_1, \{e_1, e_2\}), (p_2, \{e_3\}), (p_3, \{e_4\})\}$$



Conclusioni

Risultati ottenuti:

- Riduzione della ridondanza
- Riduzione del peso sulle risorse del sistema
- Maggiore automazione

Sviluppi futuri

- Implementazione del componente Trigger
- Implementazione degli automatismi che collegano ogni fase con la successiva
- Organizzazione dei dati per la fase manuale
- Integrazione dello schema proposto con gli schemi di certificazione esistenti

UNIVERSITÀ DEGLI STUDI
DI MILANO

Grazie per l'attenzione