La comunicazione tra oggetti pervasivi

Metodologie per rendere sicura ed anonima la trasmissione di informazioni sensibili

Prof. Pier Luca Montessoro
Ing. Davide Pierattoni
Ing. Sandro Di Giusto
DIEGM – Università degli Studi di Udine

E-privacy 2006 - Firenze
19-20 maggio

Contesto:
il pervasive computing

La prima definizione storica

> *The most profound technologies are those that disappear.*
> *They weave themselves into the fabric of everyday life until they are indistinguishable from it*
>
> Mark Weiser, *Scientific American,* September 1991

Concetti fondamentali

- Studiare modelli e tecnologie atti a fornire servizi in modo assolutamente trasparente e non invasivo
- Utilizzare “mini” o “micro” dispositivi elettronici dispersi nell’ambiente, portatili od indossabili
- Sfruttare la capacità di ricevere e trasmettere informazioni in una rete dedicata, wireless e non necessariamente strutturata

Quali applicazioni?

- Servizi alla persona
  - Car pooling pervasivo
  - Health care
  - Elder care
  - Ricerca affinità
- Servizi sul territorio
  - Controllo del territorio
  - Monitoraggio del traffico
  - Monitoraggio dell'ambiente
- …

Car Pooling

Scopo:

L'ottimizzazione e la razionalizzazione dell'uso dei mezzi privati mediante aggregazione di gruppi di persone che percorrono con regolarità uno stesso tragitto

Problemi:

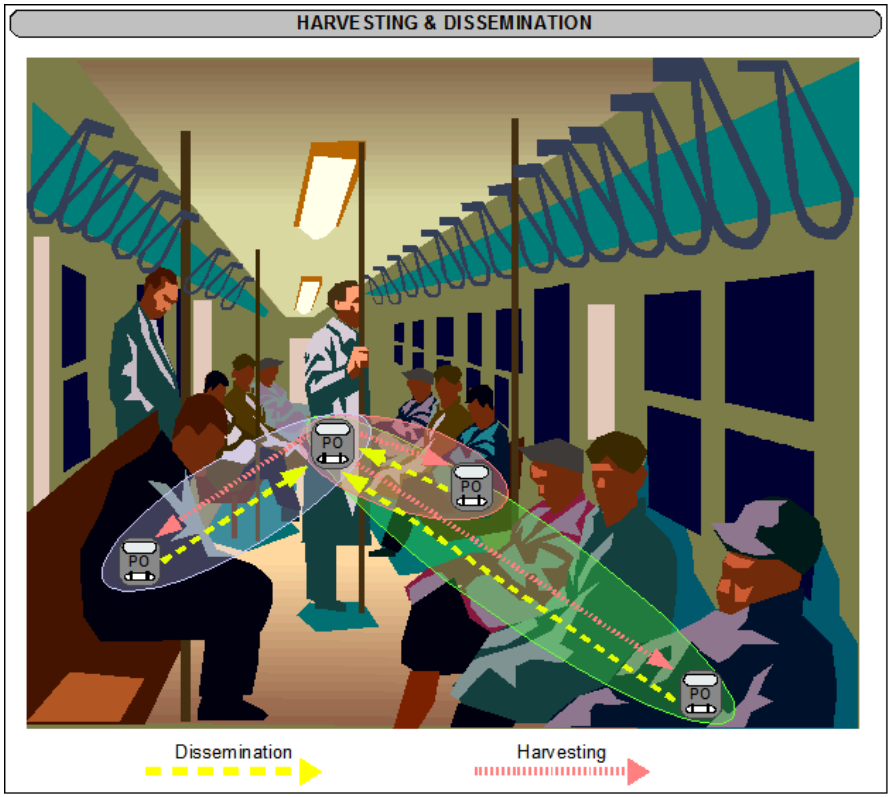
- Individuare gli utenti affini in modo efficiente
- Vincere la diffidenza degli utenti garantendo loro l'anonimato durante le ricerche di affinità
- Gestire un numero potenzialmente enorme di utenti

Pervasive Car Pooling

Dotare gli utenti di un ciondolo personale, dalle dimensioni e dai consumi trascurabili

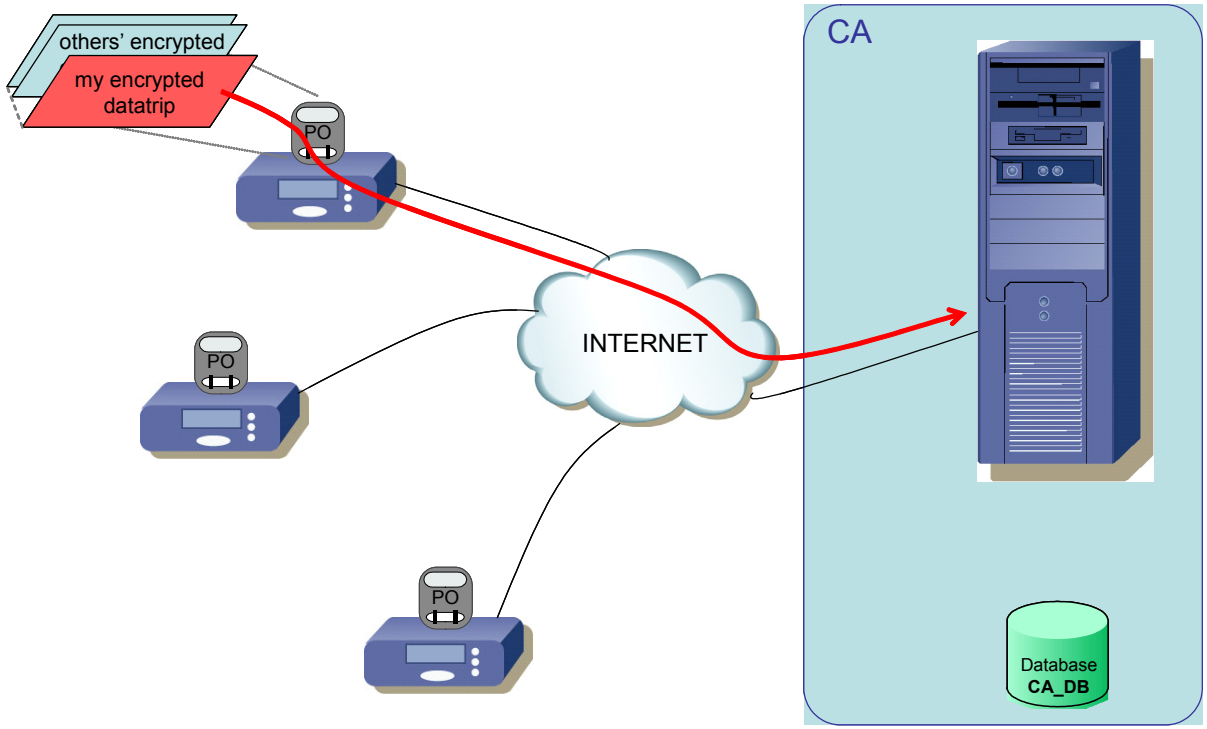
Ogni ciondolo:

- registra e pubblica i percorsi tipici (*datatrip*) del proprietario
- colleziona i percorsi ricevuti dai ciondoli degli altri utenti durante l'arco della giornata



Pervasive Car Pooling

La ricerca di affinità tra i datatrip collezionati da ciascun utente viene effettuata solo a livello centralizzato, ad opera di un'entità autorizzata e trusted



Ricerca di affinità

Scenari in cui gli utenti si affidano ad un sistema automatizzato di ricerca di affinità per conoscere altri utenti con cui condividere esperienze ed interessi

Le finalità sono ludiche o di natura sociale e il servizio viene erogato tipicamente in un'area circoscritta

Requisiti:

processare le informazioni in tempo "quasi reale" (latenze accettabili non superiori a qualche minuto) e garantire la sicurezza e l'anonimato richiesti dagli utenti

Health Care & Elder Care

Health care: servizi di monitoraggio clinico e tracciamento dello stato dei pazienti ricoverati presso una struttura sanitaria

Elder care: sistemi per il monitoraggio e l'assistenza dell'anziano nel suo ambiente di vita (casa, ospizio, …) basati su sensori ambientali

Comunicazione generalmente unidirezionale dai sensori e dispositivi biometrici verso le apparecchiature preposte alla raccolta e all'analisi di tali dati

Scenari pervasivi e riservatezza

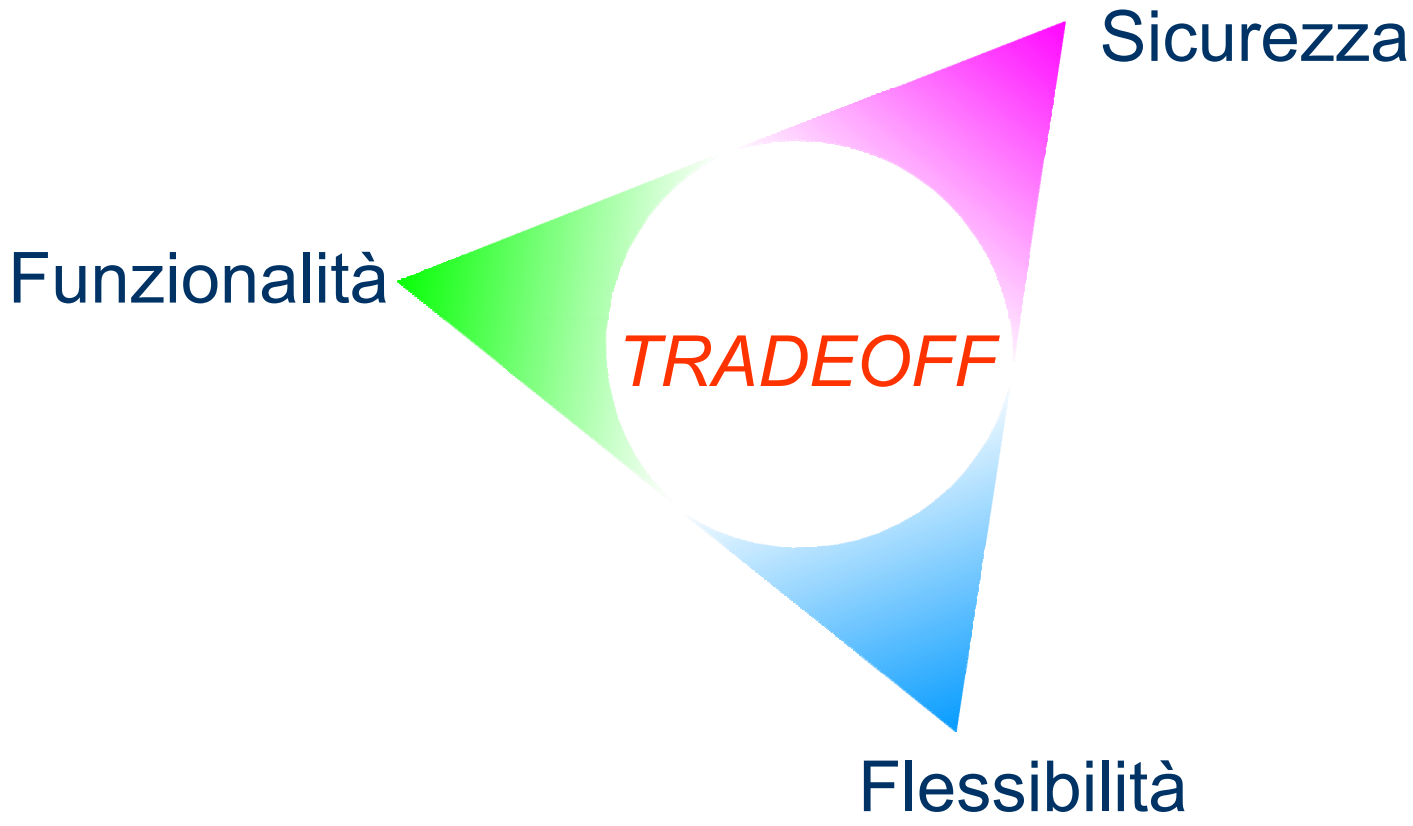
Il problema della riservatezza delle informazioni è inquadrabile sotto due aspetti:

- Autenticazione mittente e veridicità informazioni
  - E' vitale poter accertare l'autenticità dei pacchetti ricevuti e l'integrità degli stessi, così come l'autenticità del mittente e la conferma di essere il legittimo destinatario
- Divulgazione controllata e riservata ad entità accreditate
  - Le informazioni che il sistema condivide apertamente (broadcast) con il resto degli utenti non debbono poter essere decodificate ed interpretate se non dai legittimi destinatari

Una soluzione:
VPSM
Versatile Pervasive Security Model

Punti chiave

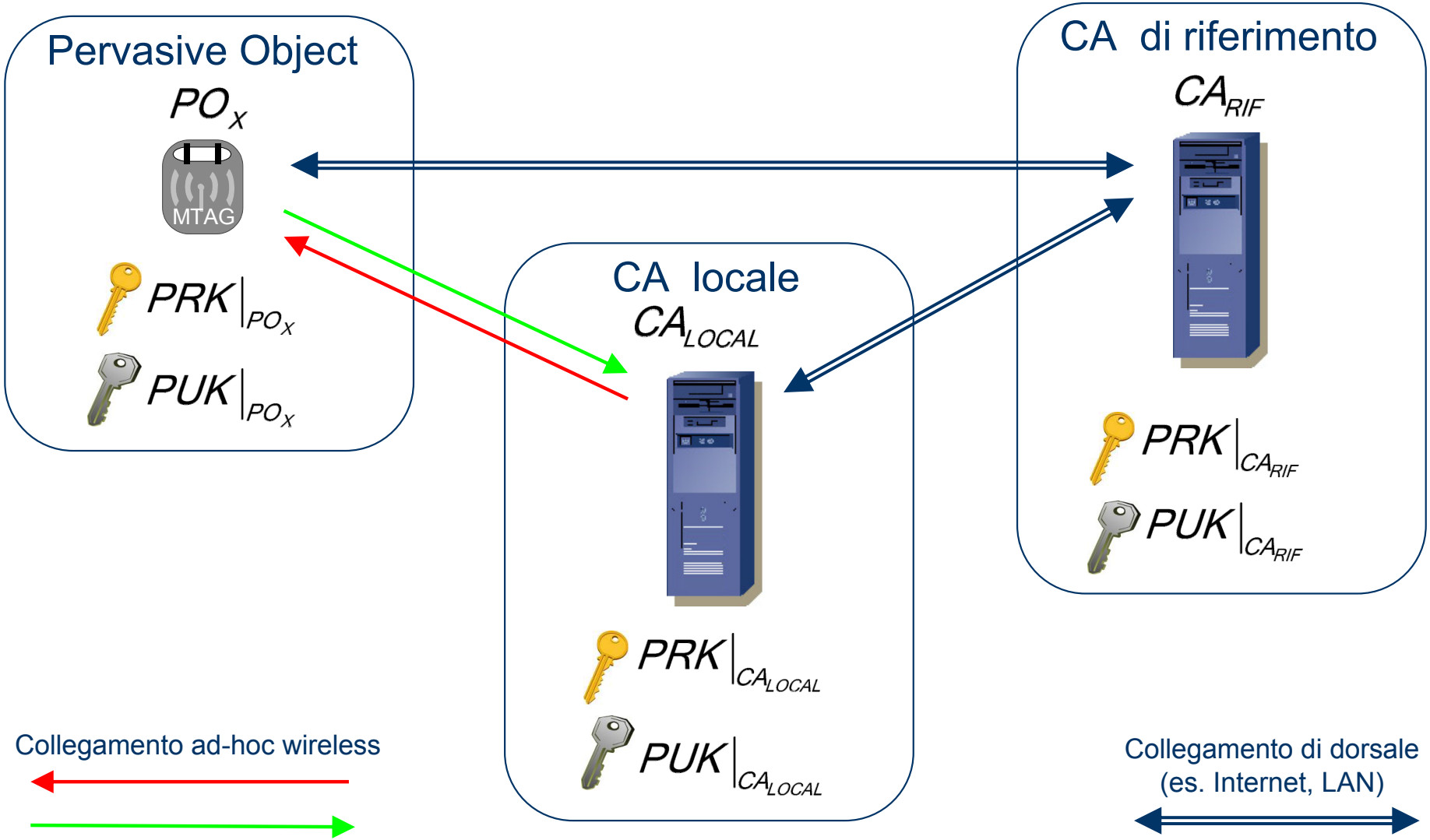
- Schema di cifratura multilivello
- Delocalizzazione dell'autorità di certificazione



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

VPSM – *Versatile Pervasive Security Model*

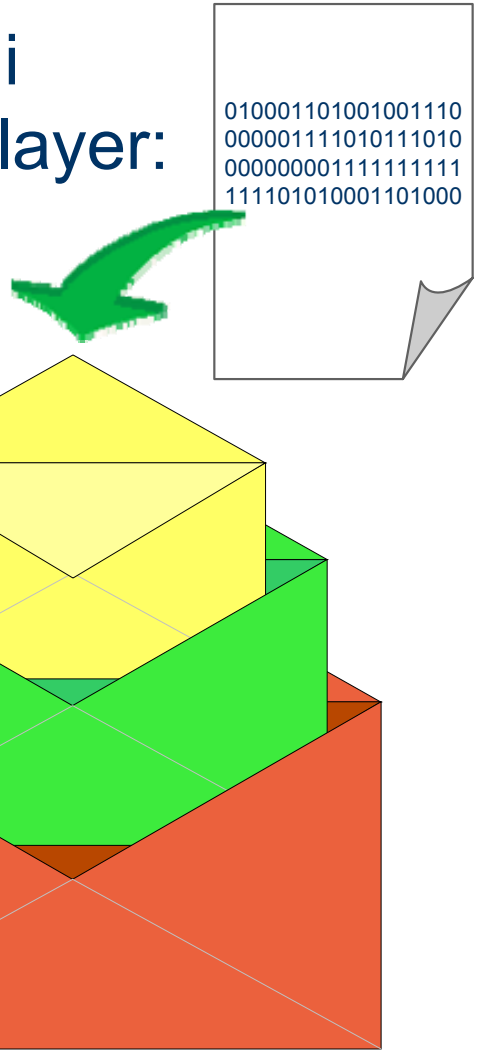
Le entità in gioco



Lo schema di cifratura multilivello

Lo stack è implementato mediante tecnica di imbustamento multiplo e si suddivide su tre layer:

3. Informazioni firmate
2. Informazioni crittografate
1. Informazioni in chiaro



Delocalizzazione dell'autorità

Esiste una gerarchia delle funzioni e delle comunicazioni tra entità

- I PO rappresentano un primo livello deputato alla raccolta ed alla disseminazione di informazioni
- Un secondo livello di comunicazione consente lo scambio delle informazioni di autenticazione tra i PO e la CA nel sistema
  - Es. ingresso e uscita dalla rete, gestione dei gruppi

Più le operazioni necessarie alla decodifica, quest'ultima ad opera della CA

Organizzazione dell'autorità

In aggiunta ai due livelli gerarchici di gestione delle comunicazioni PO⇔PO e PO⇔CA, esiste un livello gerarchico parallelo per quanto riguarda la gestione CA⇔CA, ovvero la *federazione delle autorità*.

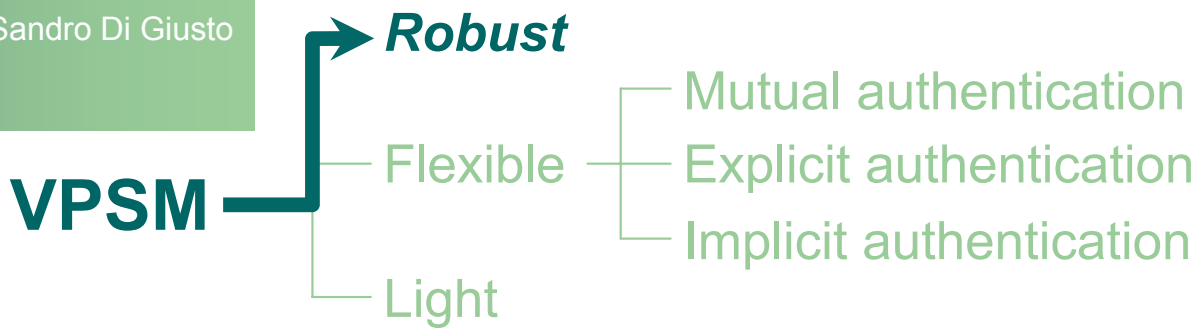
- completamente trasparente agli utenti ed agli oggetti pervasivi
- garantisce possibilità virtualmente illimitate di scalabilità
- permette di ottenere livelli di privacy e di sicurezza difficilmente realizzabili in sistemi non federati

Diverse esigenze ⇨ diverse varianti

☞ Il modello presentato si diversifica in base alle esigenze del servizio ed alle disponibilità tecniche dello scenario in cui è chiamato ad operare

☞ Sono state realizzate quindi tre varianti distinte dello stesso modello VPSM

- Robust
- Flexible
  - Mutual authentication
  - Explicit authentication
  - Implicit authentication
- Light



Target:

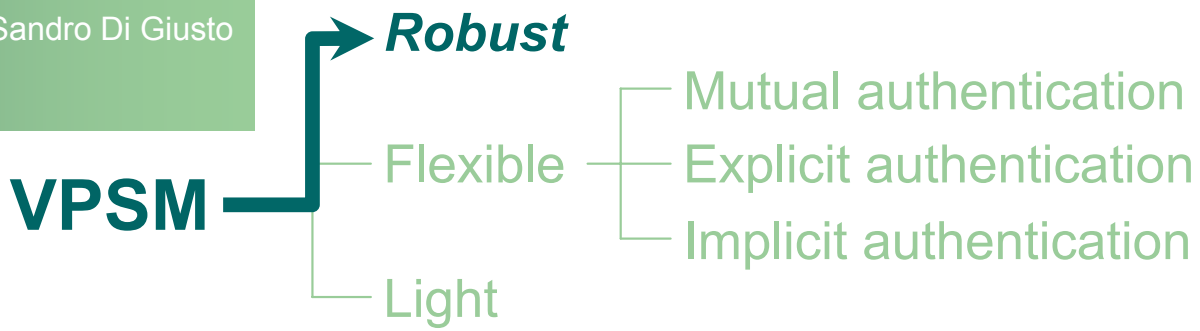
Scenari non real-time, dove non si necessita di rapidità nello scambio di informazioni

I nodi si occupano esclusivamente di disseminare e raccogliere informazioni che non elaborano

- Unidirezionalità totale dei flussi PO→CA

L'accesso alla CA da parte degli oggetti pervasivi è oggettivamente sporadico

- *Car pooling pervasivo*

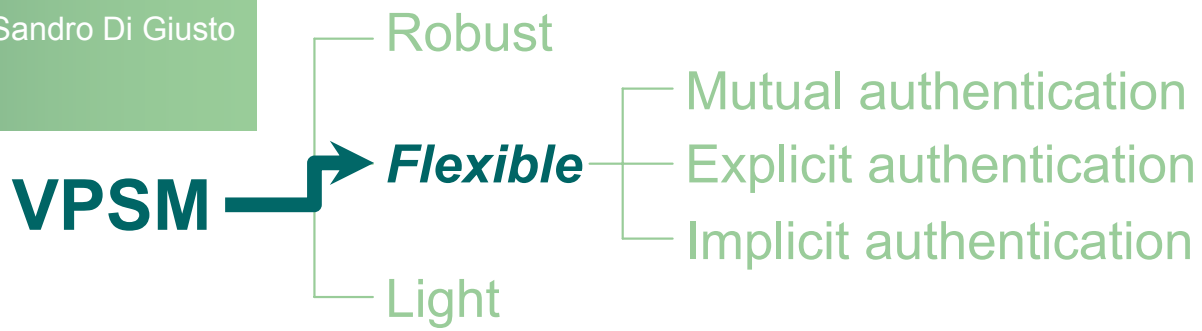


Pro:

- Sicurezza e garanzia di anonimato
- Bassi requisiti HW e SW nei PO (delegabili alle interfacce di gestione e comunicazione con la CA, ad esempio i PC)
- Scalabilità tramite *federazione* di CA

Contro:

- Non permette comunicazioni “on the fly” tra PO né tra PO e CA
- A seconda degli scenari, può richiedere nei PO un discreto quantitativo di memoria per lo storage dei dati raccolti (*harvesting*)
- Richiede un’interfaccia esterna:
  - per la gestione delle informazioni da far condividere al PO
  - per far comunicare il PO con la propria CA di riferimento tramite un canale di comunicazione dedicato



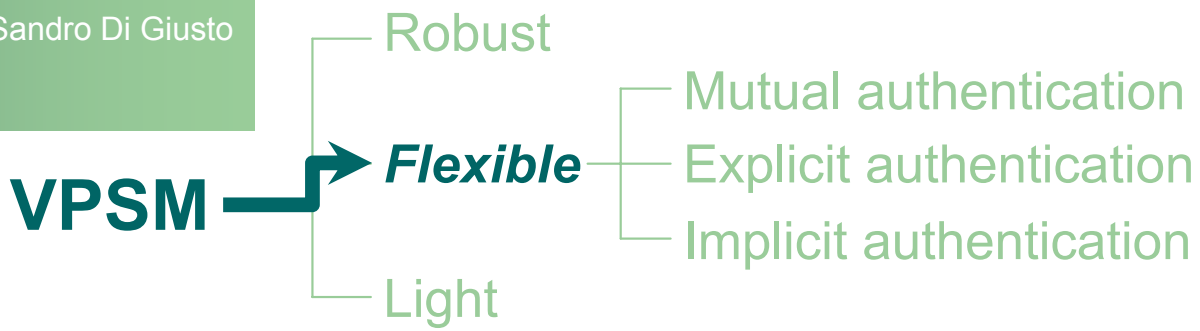
Target:

Scenari che richiedono una comunicazione “nearly on the fly” (latenze medio-basse) e flessibilità

- *Ricerca di affinità*
- *Health care & Elder care*
- *Sensoristica*

Caratteristiche:

- elevata sicurezza e buon livello di anonimato
- prevede un’entità di autenticazione locale (*CA locale*) ed eventualmente una centrale (*CA di riferimento*)

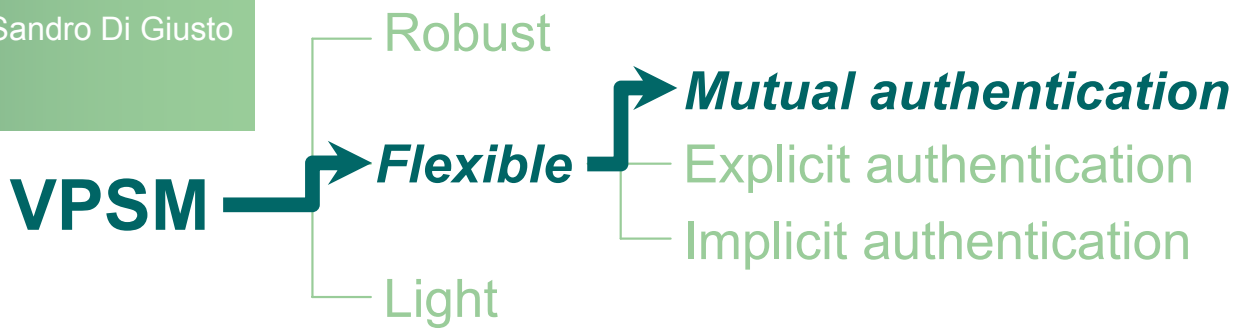


Protocolli:

La flessibilità di questa variante è legata strettamente al fatto che possono esistere diversi schemi di autenticazione, a seconda delle caratteristiche dello scenario in cui si opera

Sono stati studiati tre protocolli di autenticazione:

- Mutual authentication
- Explicit authentication
- Implicit authentication



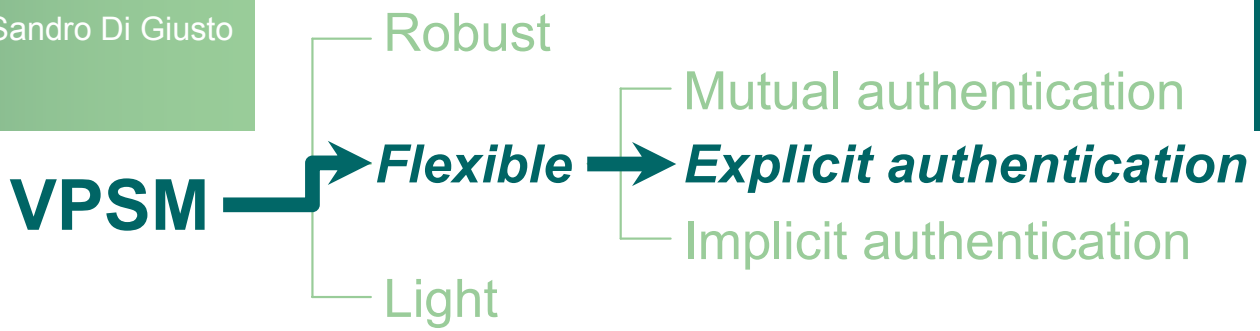
Prevede che nel processo iniziale di "*discovery*" fra un oggetto e la CA locale, entrambe siano autenticate da una terza entità di garanzia, ovvero la CA di riferimento

Pro:

- Sicurezza e ottimo livello di garanzia di anonimato
- Permette di ottenere latenze piuttosto basse
- Scalabilità tramite federazione di CA

Contro:

- Richiede link attivo tra CA locale e CA di riferimento



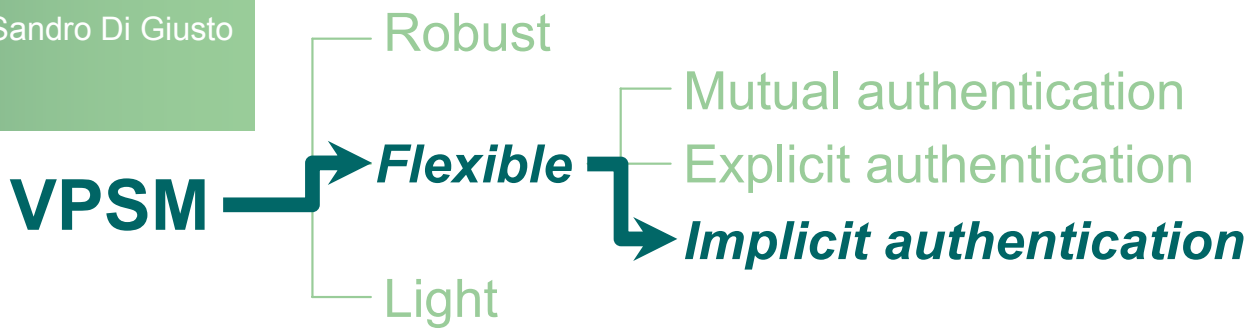
La fase di "*discovery*" tra PO e CA locale prevede autenticazione esplicita (non trasparente) ed in un solo verso: il PO autentica la CA locale sulla base della propria localizzazione oppure dialogando con una CA *di prossimità* che gestisce ingressi e uscite nel sistema

Pro:

- Buona sicurezza e ottimo livello di garanzia di anonimato
- Permette di ottenere latenze basse
- Non necessita della CA di riferimento né di link permanenti

Contro:

- La CA locale non può autenticare il PO
- Il protocollo non è completamente trasparente per l'utente
- E' adatto per servizi erogati in ambienti confinabili



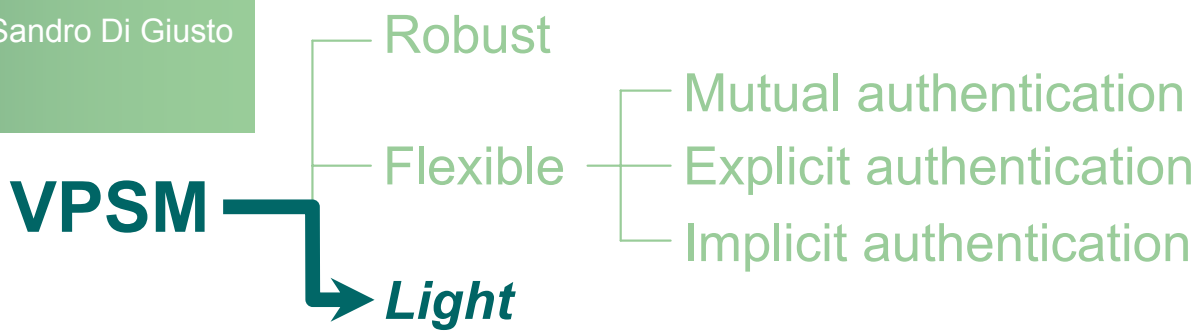
La fase di "*discovery*" tra PO e CA locale si basa sull'universalità dei parametri di sicurezza delle CA locali: ogni CA locale è implicitamente autenticata per il fatto che risponde alla configurazione standard di sicurezza nota a priori ai PO.

Pro:

- Discreta sicurezza e discreta garanzia di anonimato
- Permette di ottenere latenze basse
- Non necessita della CA di riferimento né di link permanenti

Contro:

- La CA locale non può autenticare il PO
- L'universalità dei parametri di sicurezza del CA locale è critica e si presta solo per piccoli sistemi ben delimitabili

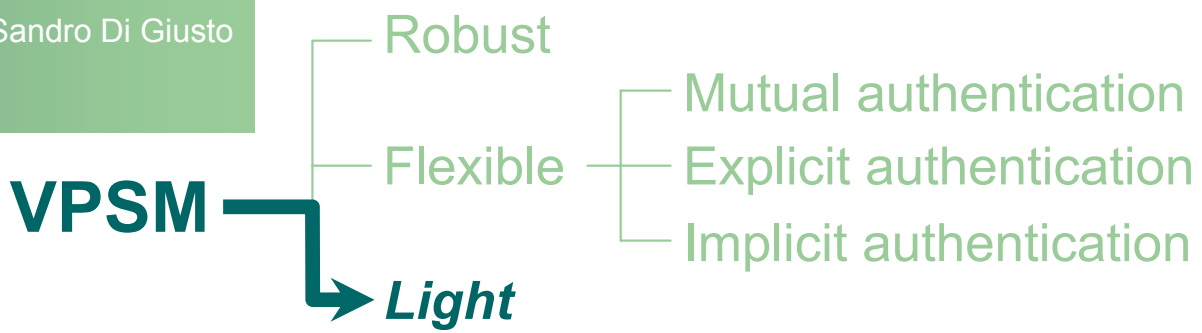


Target:

Scenari in cui la leggerezza del protocollo e del carico computazionale per i PO è prioritario, così come la semplicità dell'infrastruttura delle CA.

Rappresenta un compromesso per quei particolari servizi in cui si può garantire l'autenticazione degli utenti attraverso altri canali, oppure in cui l'autenticazione non è necessaria a livello di comunicazione

- controllo/registrazione di accessi



Pro:

- Semplicità del protocollo
- Basso carico computazionale
- Bassa complessità dell'infrastruttura delle CA
- Non necessita della CA di riferimento né di link permanenti

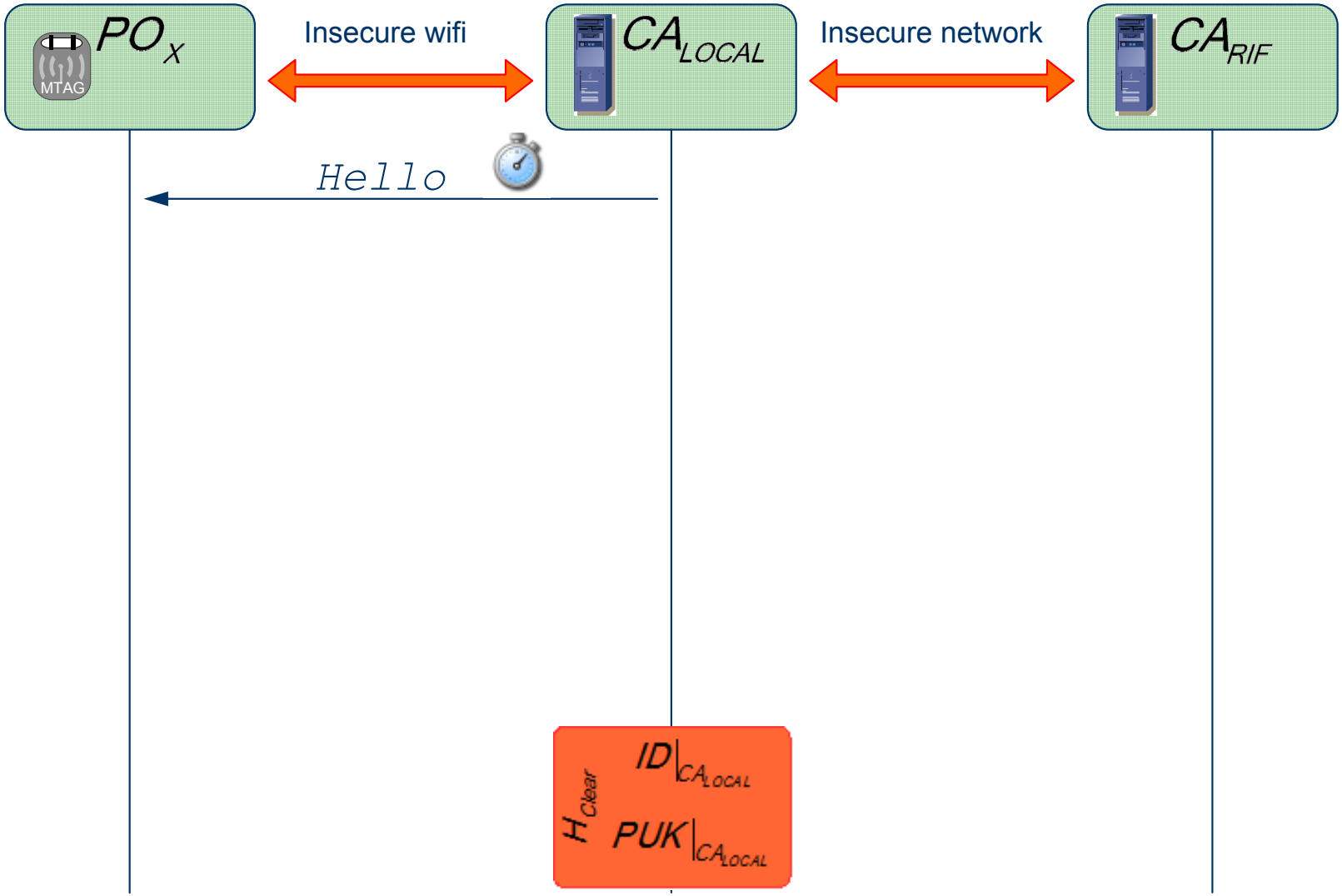
Contro:

- Non prevede alcuno scambio di messaggi di autenticazione
- La privacy non è garantita
- Occorre prevedere una forma alternativa di autenticazione degli utenti che non utilizzi il canale di comunicazione

Schema di dettaglio: Flexible with Mutual authentication

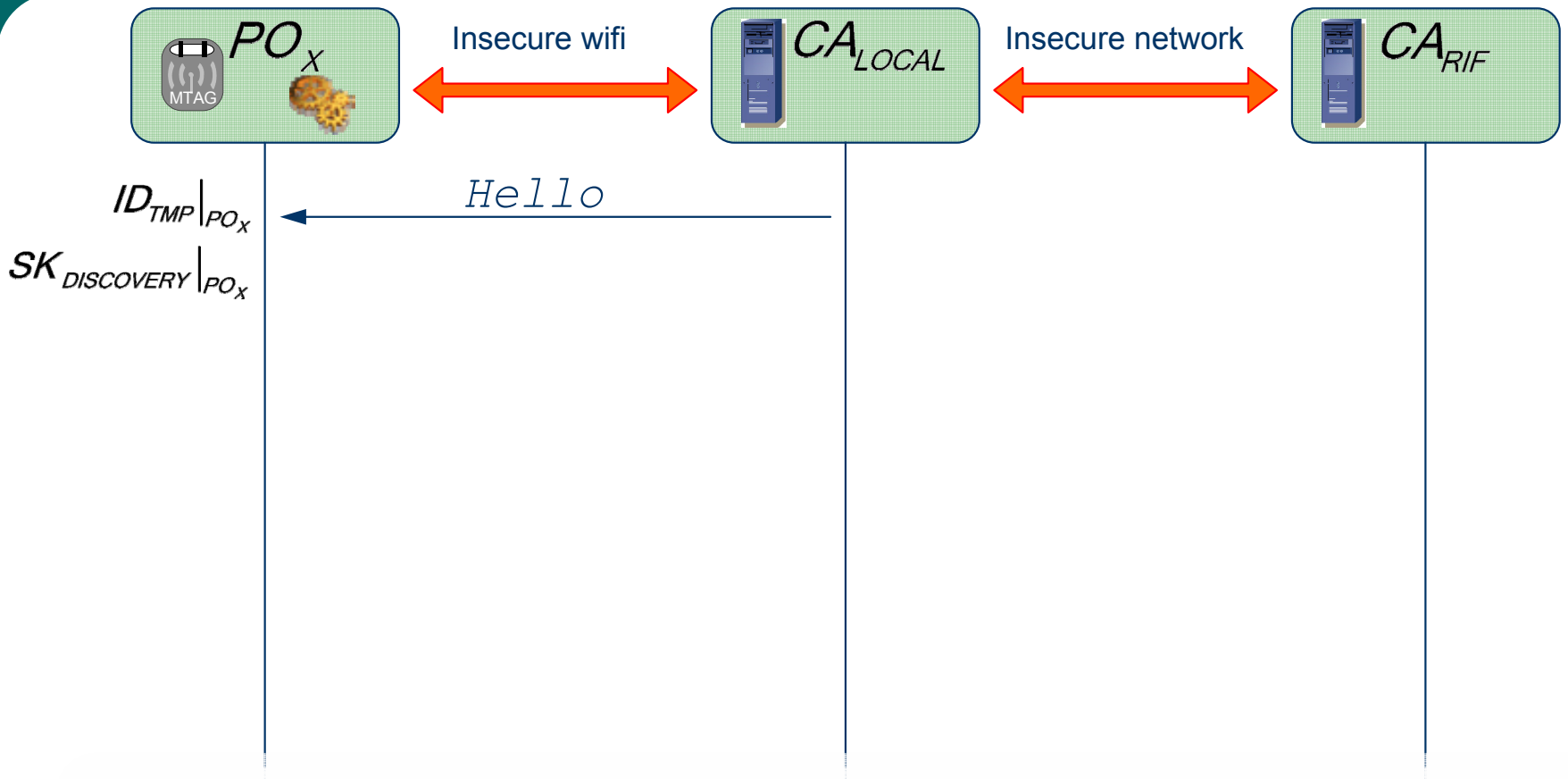
Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication

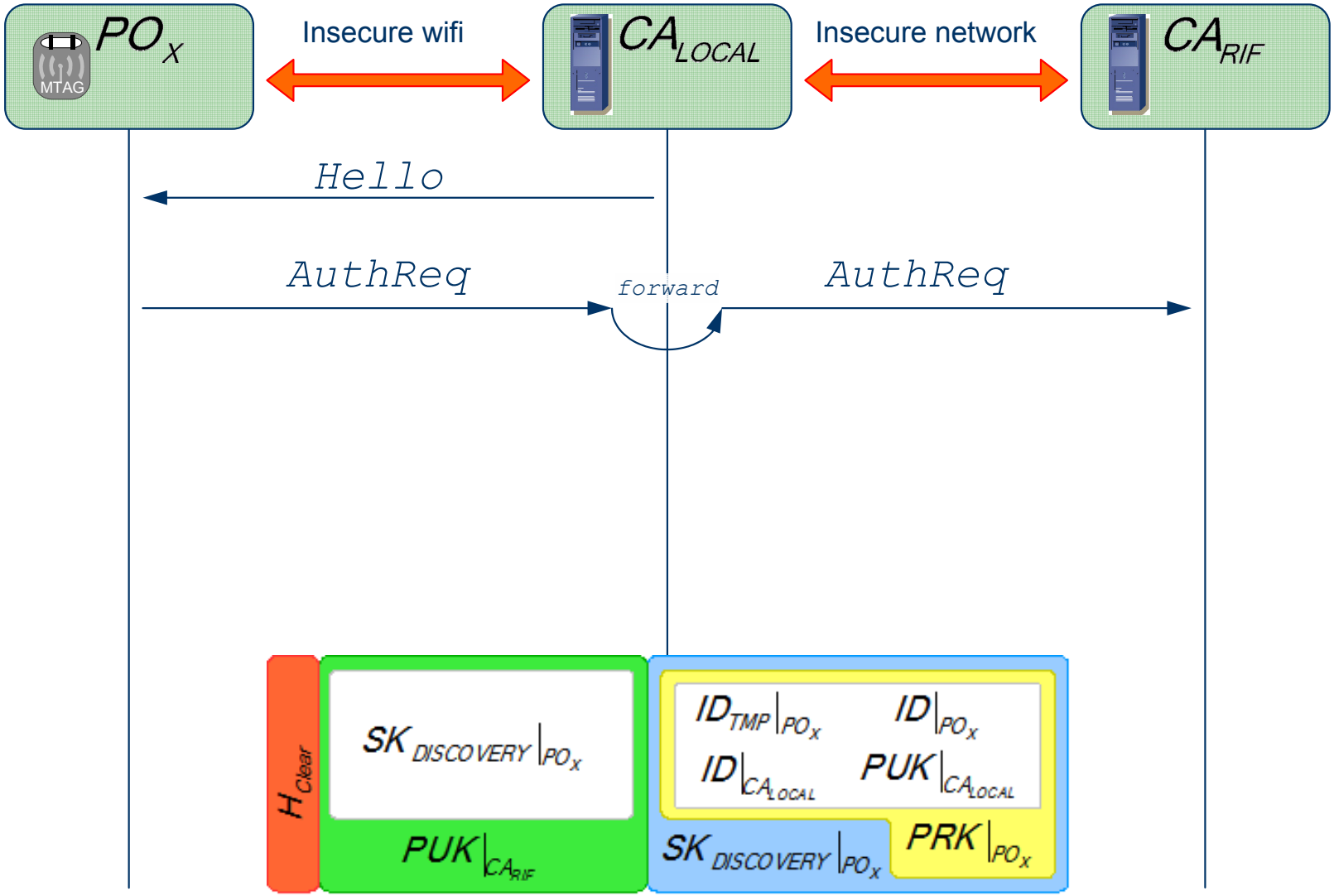


Vengono generati al volo due valori casuali:

- Un identificativo pseudo-univoco temporaneo (anonimato)
- Una chiave simmetrica di *discovery* (sicurezza)

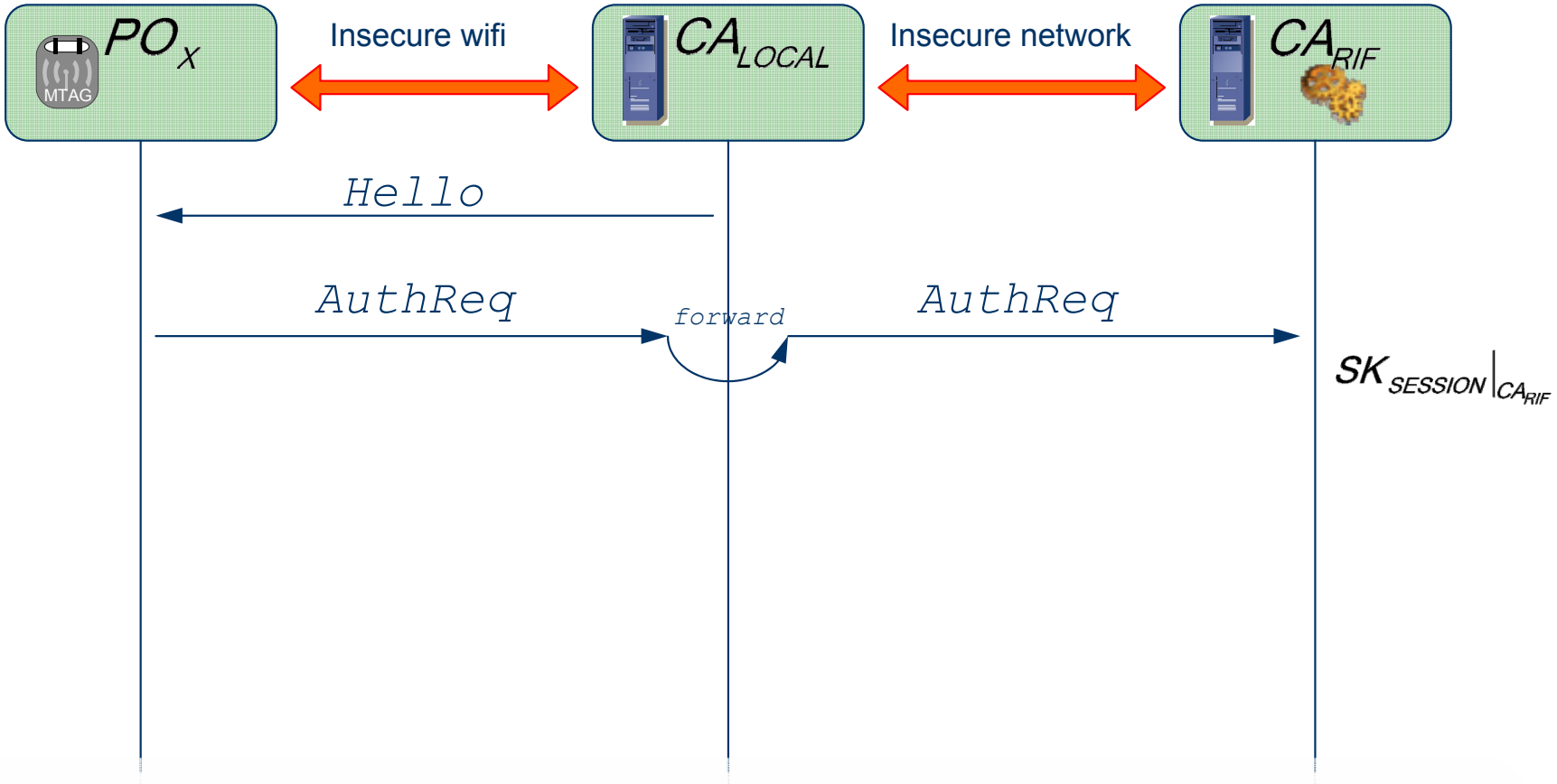
Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

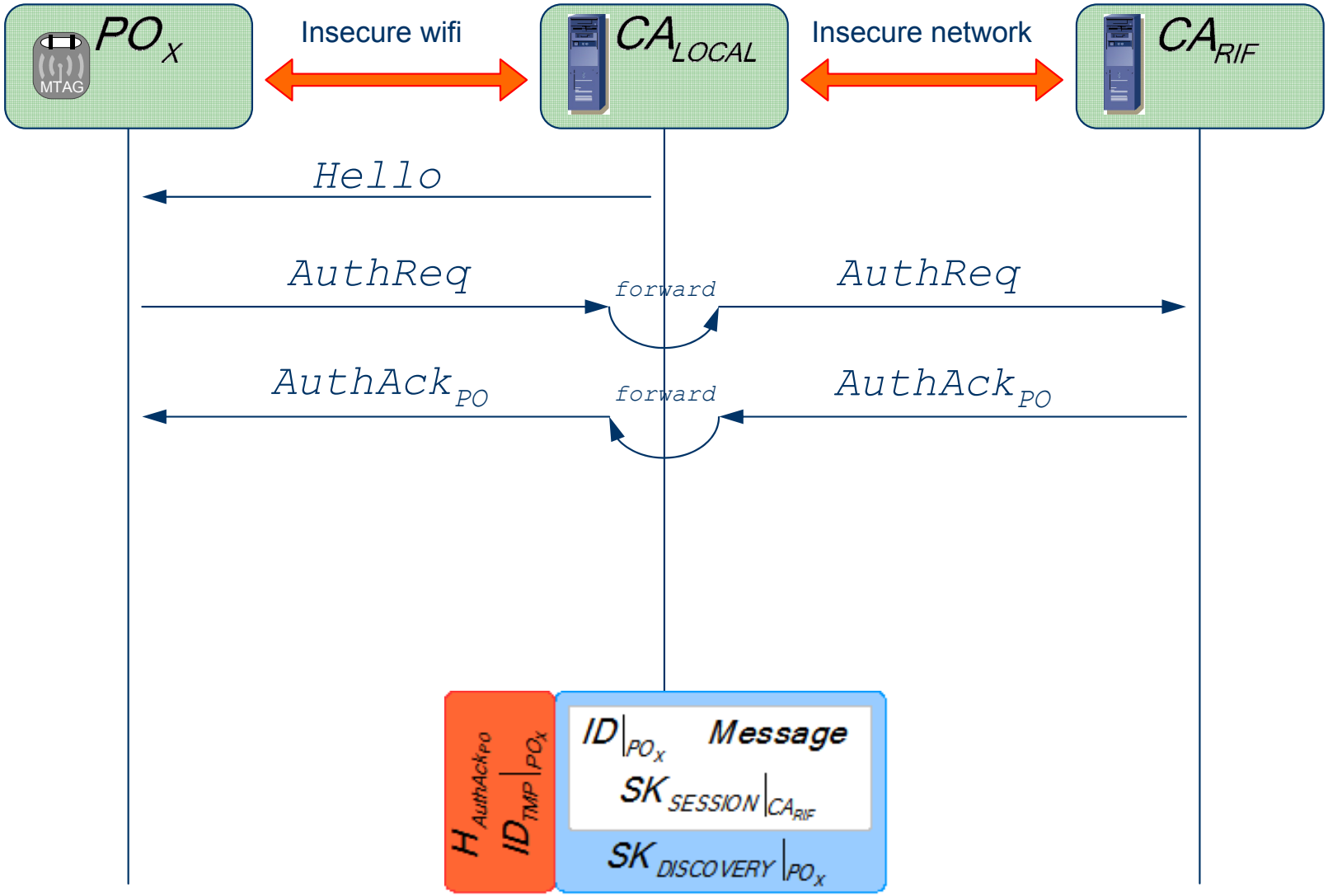
Flexible : Mutual authentication



- Verifica esistenza e autenticità di PO_X nel proprio DB
- Verifica esistenza e coerenza di CA_{LOCAL} nel proprio DB
- Genera una chiave temporanea di sessione $SK_{SESSION}|_{CA_{RIF}}$

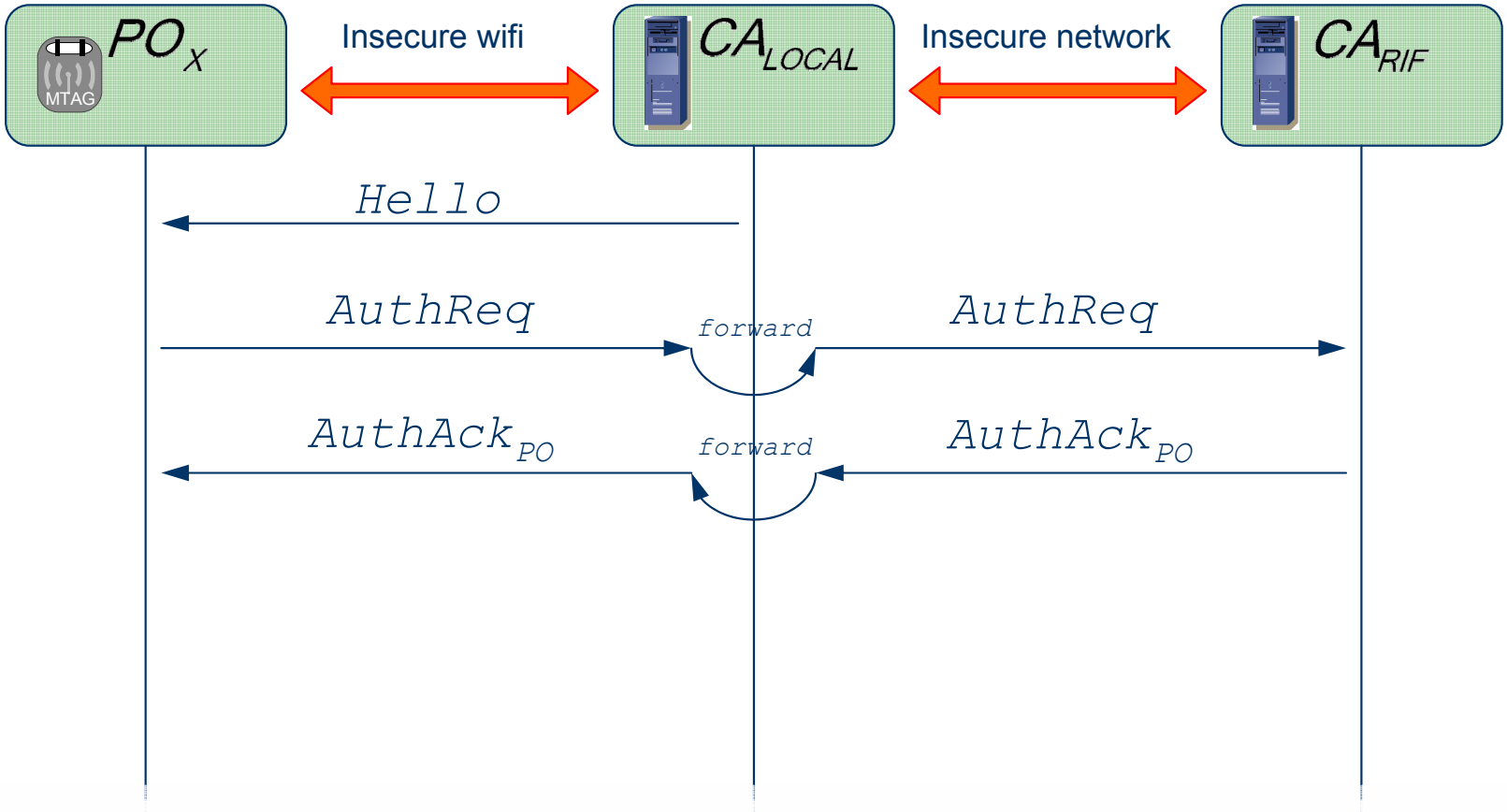
Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication

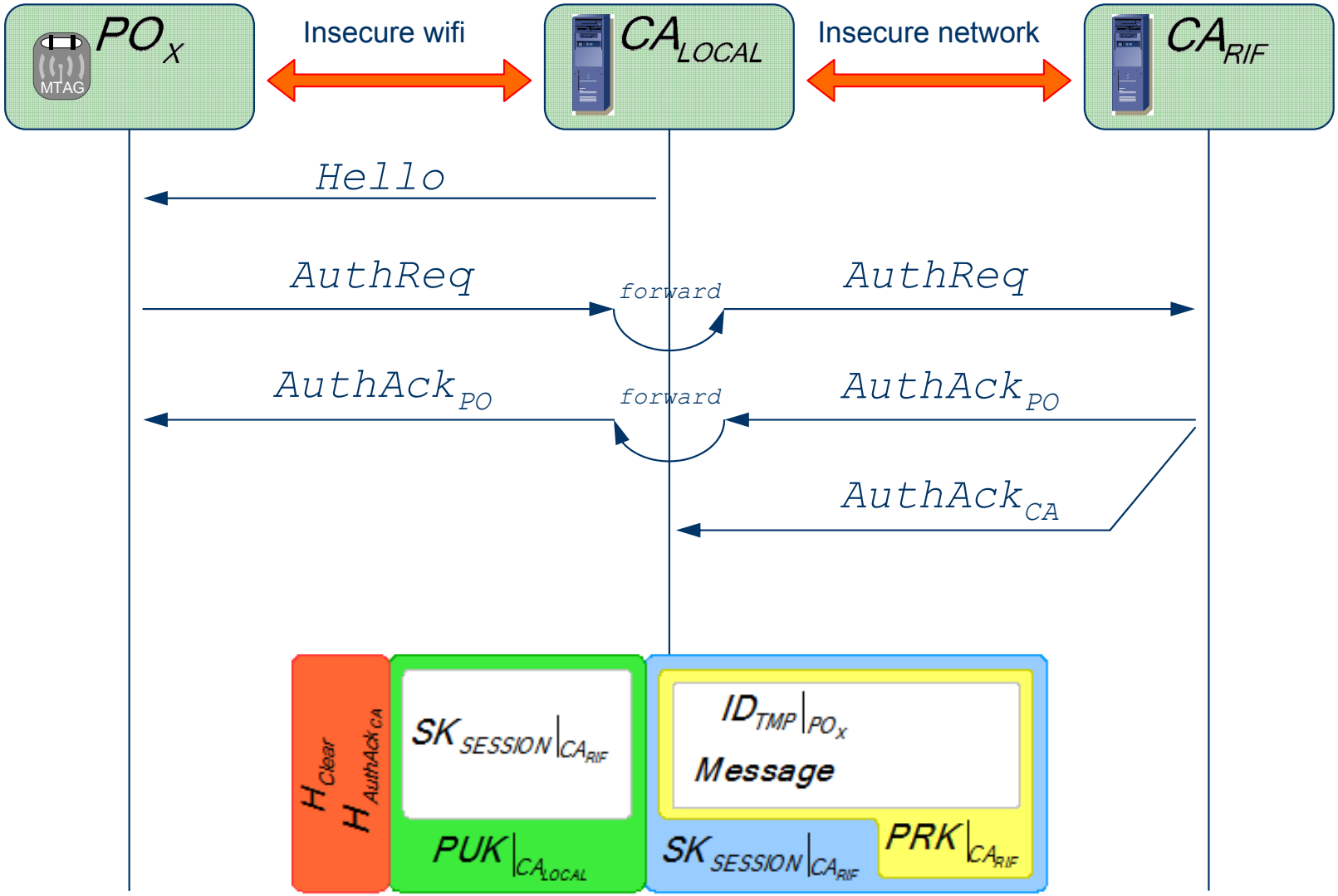


PO_X capisce d'essere il destinatario grazie a $ID_{TMP}|_{PO_X}$

- Comprende che CA_{LOCAL} è un *CA* fidato
- Memorizza la nuova chiave simmetrica di sessione $SK_{SESSION}|_{CA_{RIF}}$

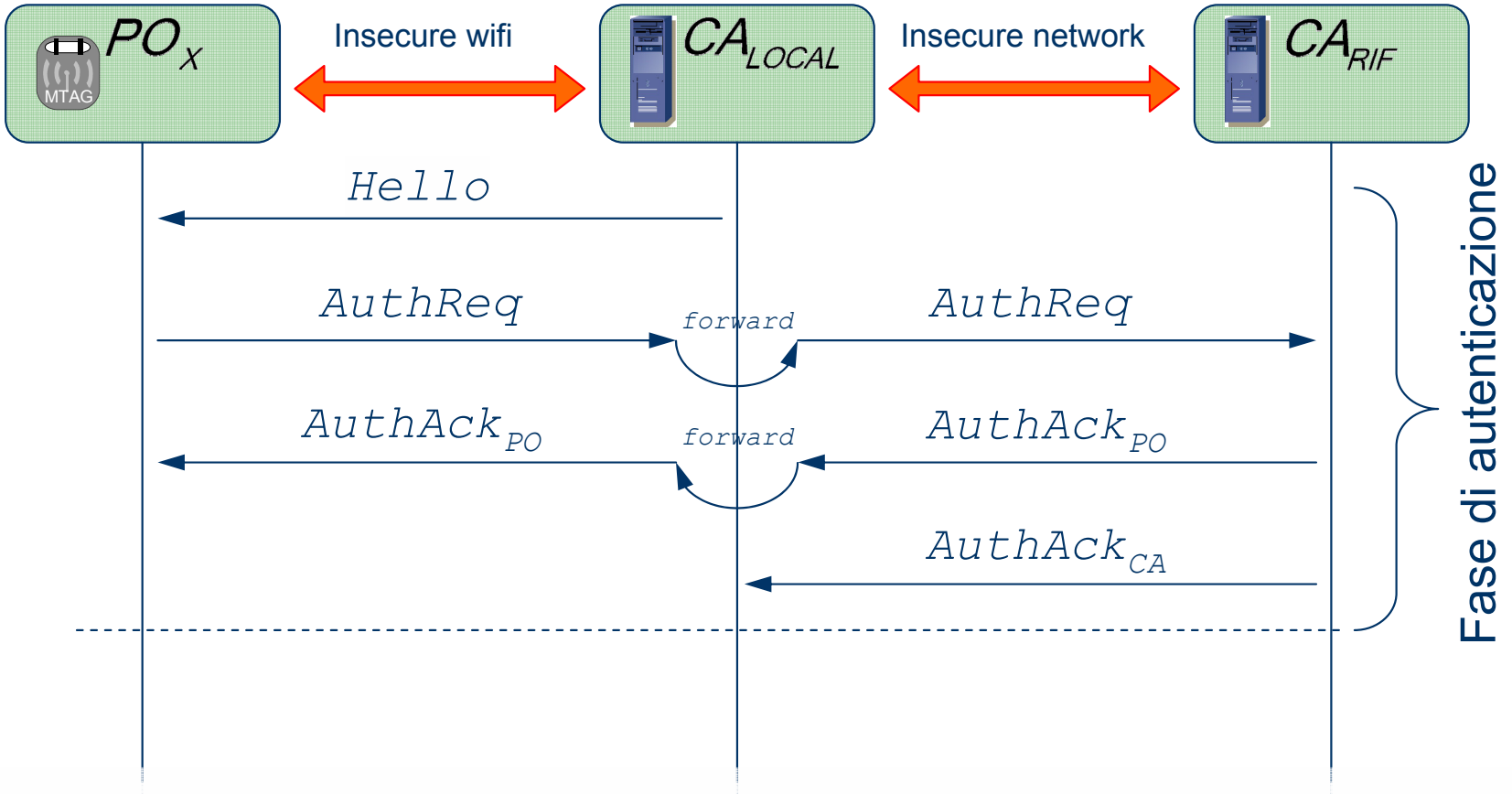
Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

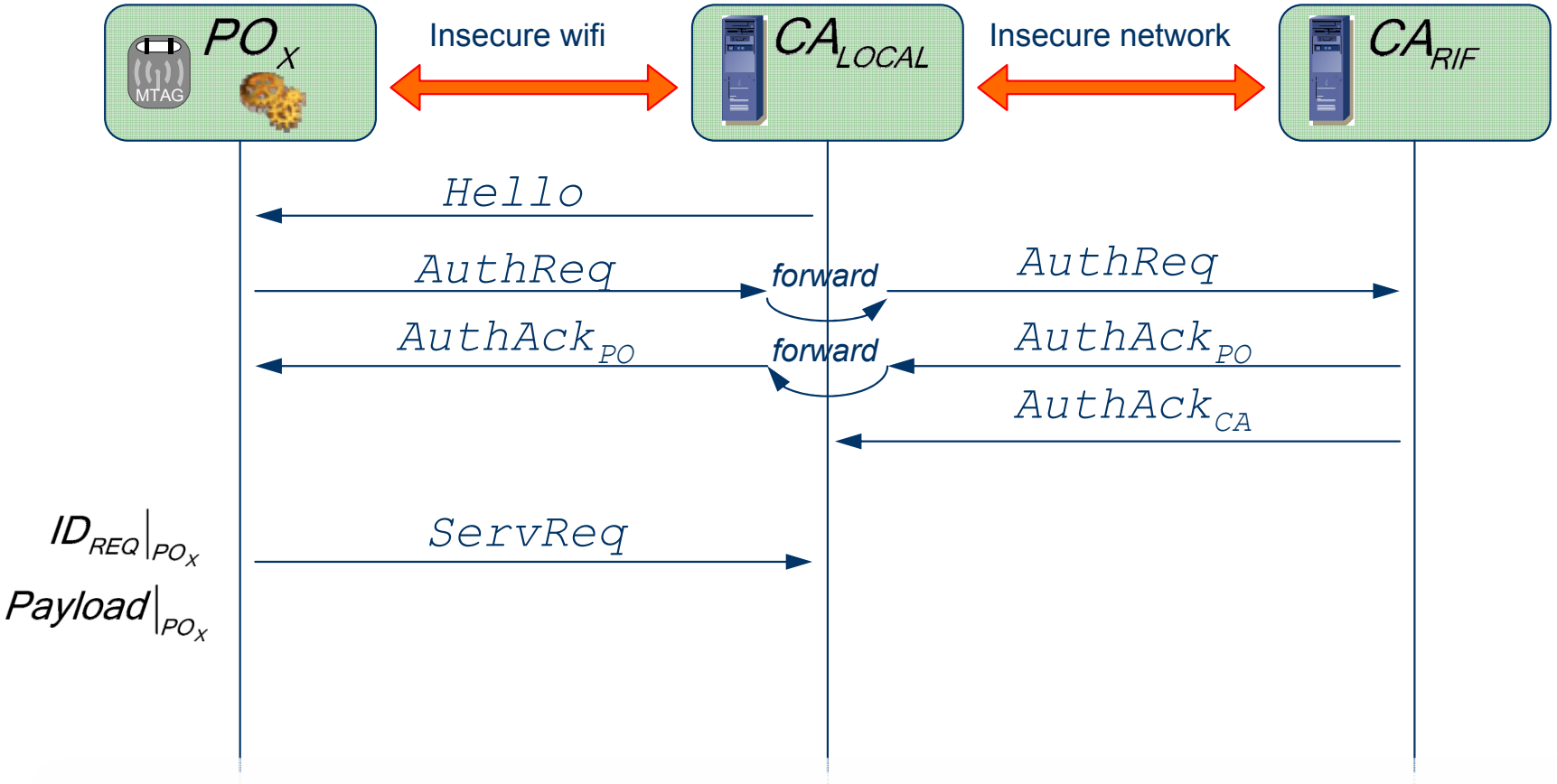
Flexible : Mutual authentication



La fase di autenticazione è terminata con successo.
Il PO_X è ora in grado di comunicare in totale anonimato e sicurezza con il CA_{LOCAL} senza l'ausilio di CA_{RIF} né della rete – *Fase di dialogo*

Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

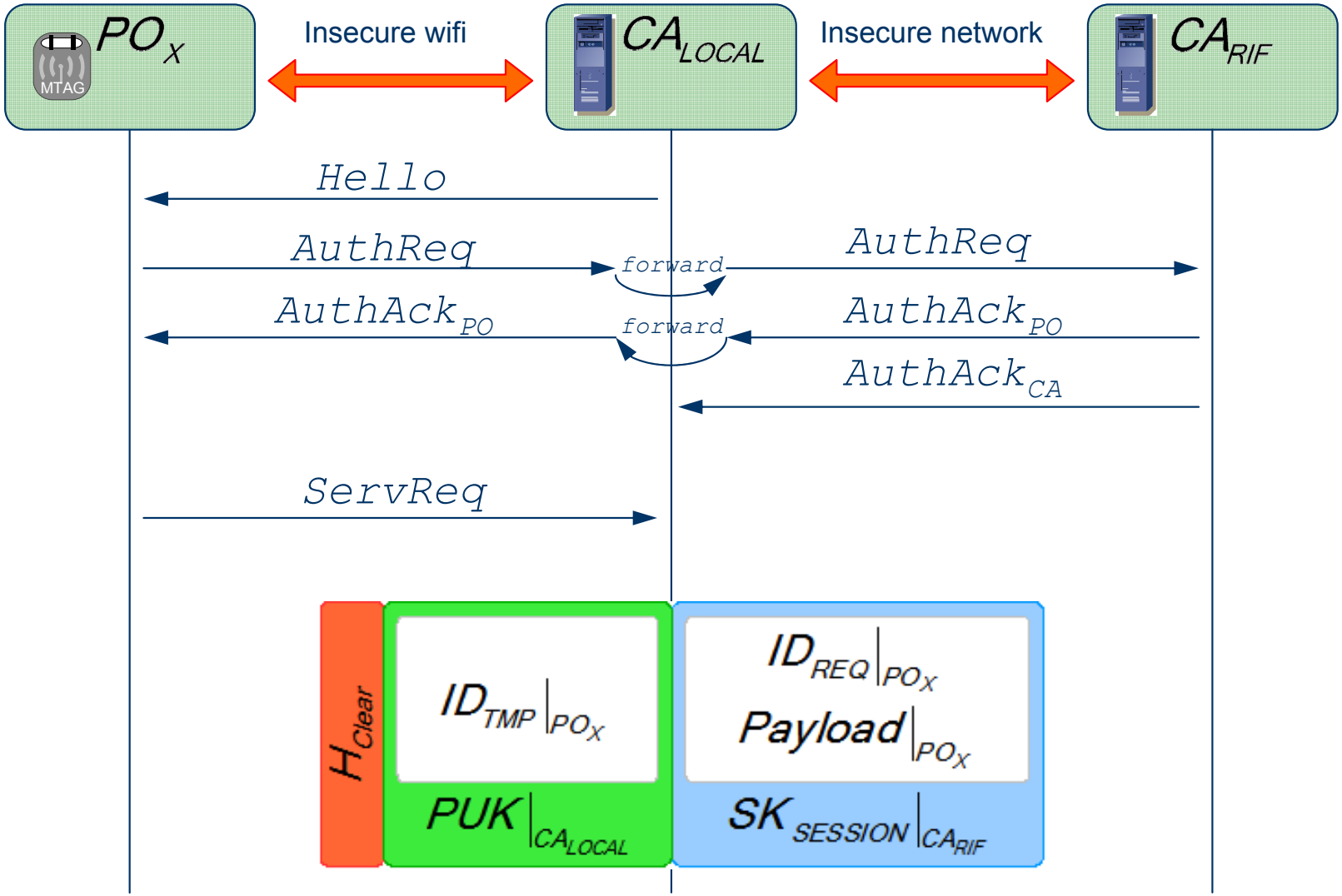
Flexible : Mutual authentication



Quando il PO_X necessita di inviare informazioni, genera un identificativo di richiesta casuale $ID_{REQ}|_{PO_X}$ ed invia la richiesta

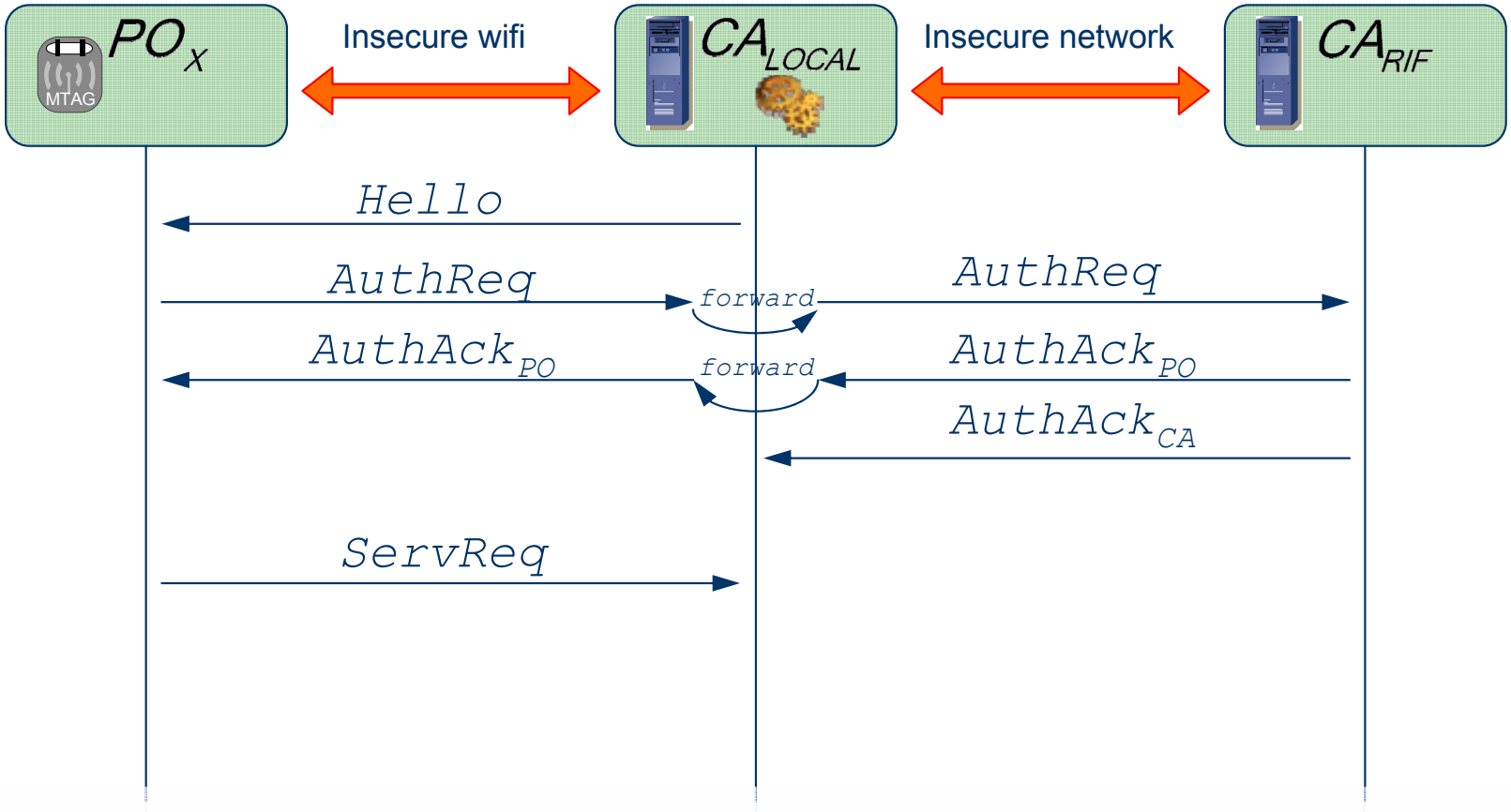
Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

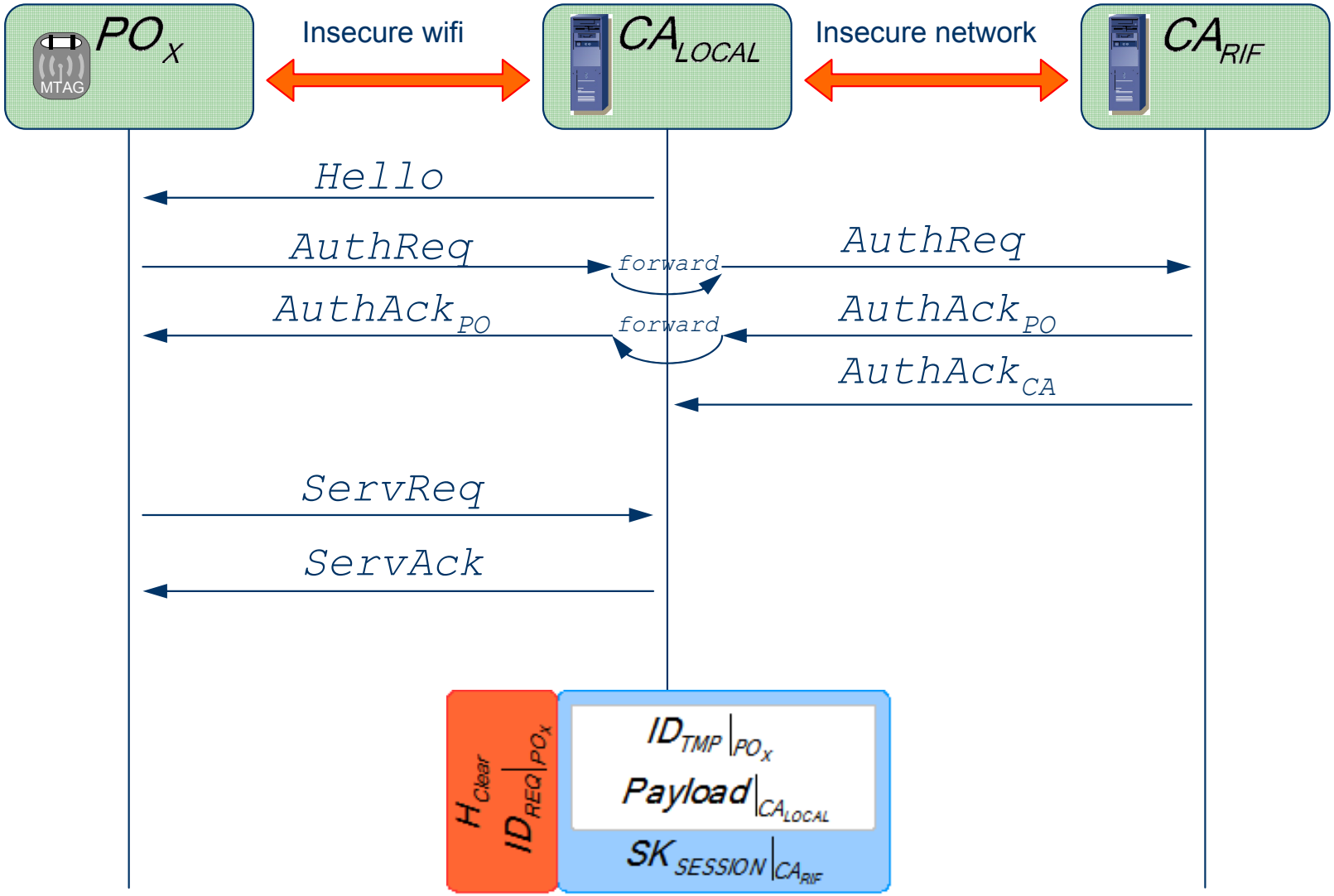
Flexible : Mutual authentication



CA_{LOCAL} ha ricevuto la richiesta di servizio ed elabora la risposta (se prevista) secondo lo scenario applicativo in cui opera

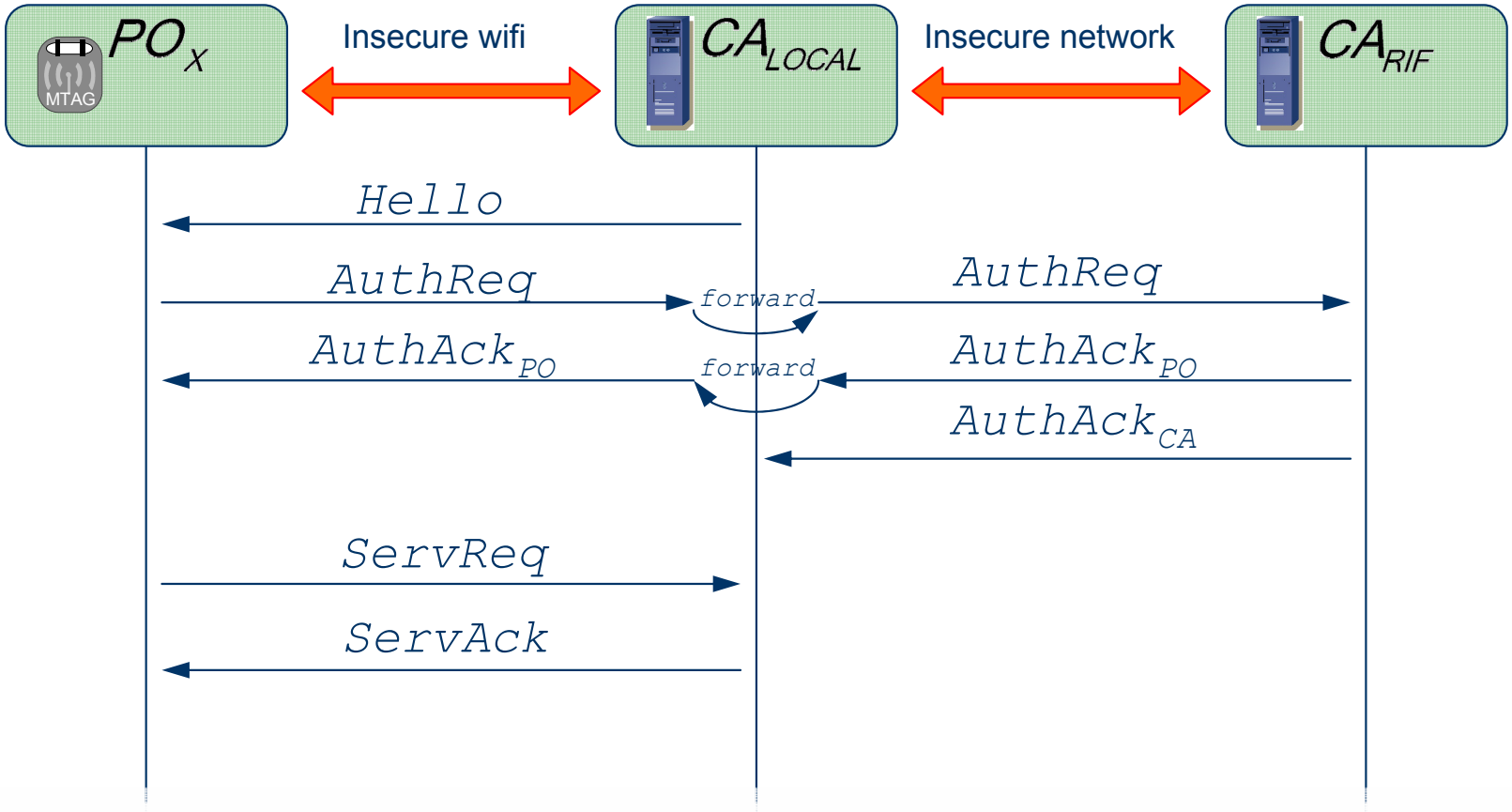
Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



Pier Luca Montessoro, Davide Pierattoni, Sandro Di Giusto
DIEGM – Università degli Studi di Udine

Flexible : Mutual authentication



- PO_X ha ricevuto la risposta (ove prevista) in maniera sicura e completamente anonima
- L'operazione può essere ripetuta indefinitamente

Conclusioni

Conclusioni

- VPSM integra in un framework comune le tecnologie standard odierne e future applicabili nel pervasive computing
  - Crittografia e algoritmi
  - Infrastrutture di comunicazione wired e wireless
  - Sistemi per l'identificazione e la localizzazione
- Il contenuto innovativo di VPSM risiede nella formalizzazione della metodologia e nella generalità degli schemi proposti