# Establishing Trust Across Zones in NDN: Challenges and Design Considerations

Adriana V Ribeiro, André Luiz R Madureira, Leobino N Sampaio
Federal University of Bahia, Brazil

NDN Community Meeting 2025 (NDNComm 2025) - 2025 04 18

# Our team

- Prof. Dr. Leobino Sampaio
  - UFBA's Associate Professor Computer Science Department
  - > 20 yrs focused in Internet technologies
  - Visiting researcher (sabbatical) - UCLA (2020)

- Adriana Viriato Ribeiro
  - PhD student in Computer Science
  - Visiting scholar - UCI (2022 - 2023)
  - Thesis investigation: Community-scale IoT communications through future Internet architectures

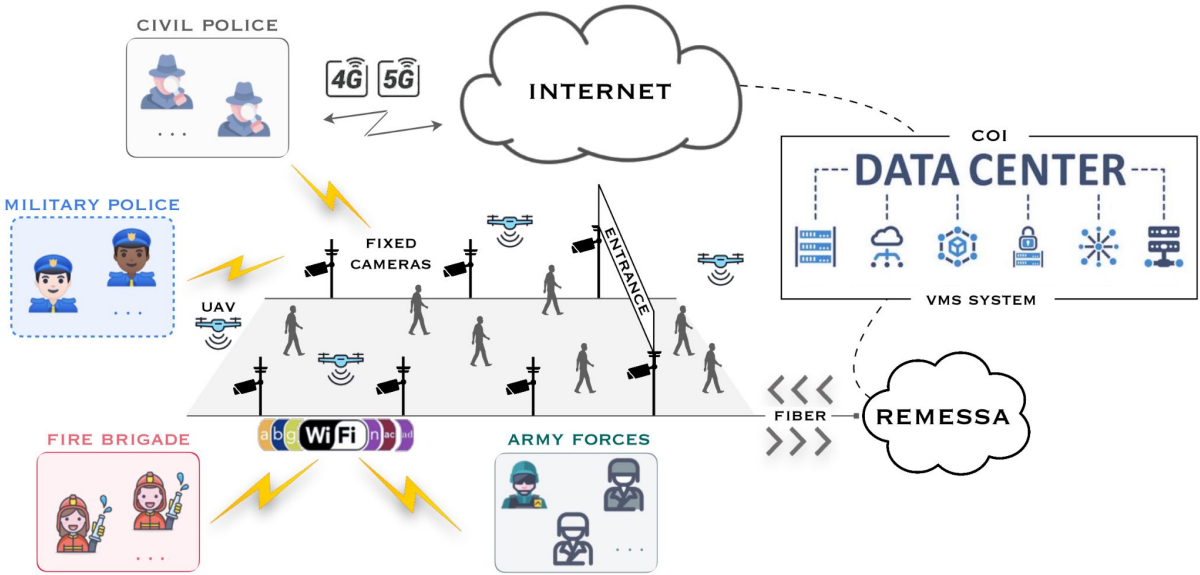
- André Madureira
  - PhD student in Computer Science
  - Visiting B.S. student at University of Georgia (2014 - 2015)
  - Thesis investigation: Congestion control of Mobile NDN-IoT communications

# Use case: Salvador Carnival

- A public and free festivity organized by the Salvador City Hall and the state government during seven days
- Number of people: 11 millions in 2025
- An important requirement: granting public order and safety
  - Integrated coordination of security representatives of independent institutions with their IT governance
  - More than 30,000 security professionals working together
  - Military and Civil Police, Fire Brigade, and Army forces
  - Devices: stationary devices (i.e., fixed cameras), slow-moving devices (i.e., wearables and cameras installed in the custom cars), and moderate-moving devices (i.e., flying drones)

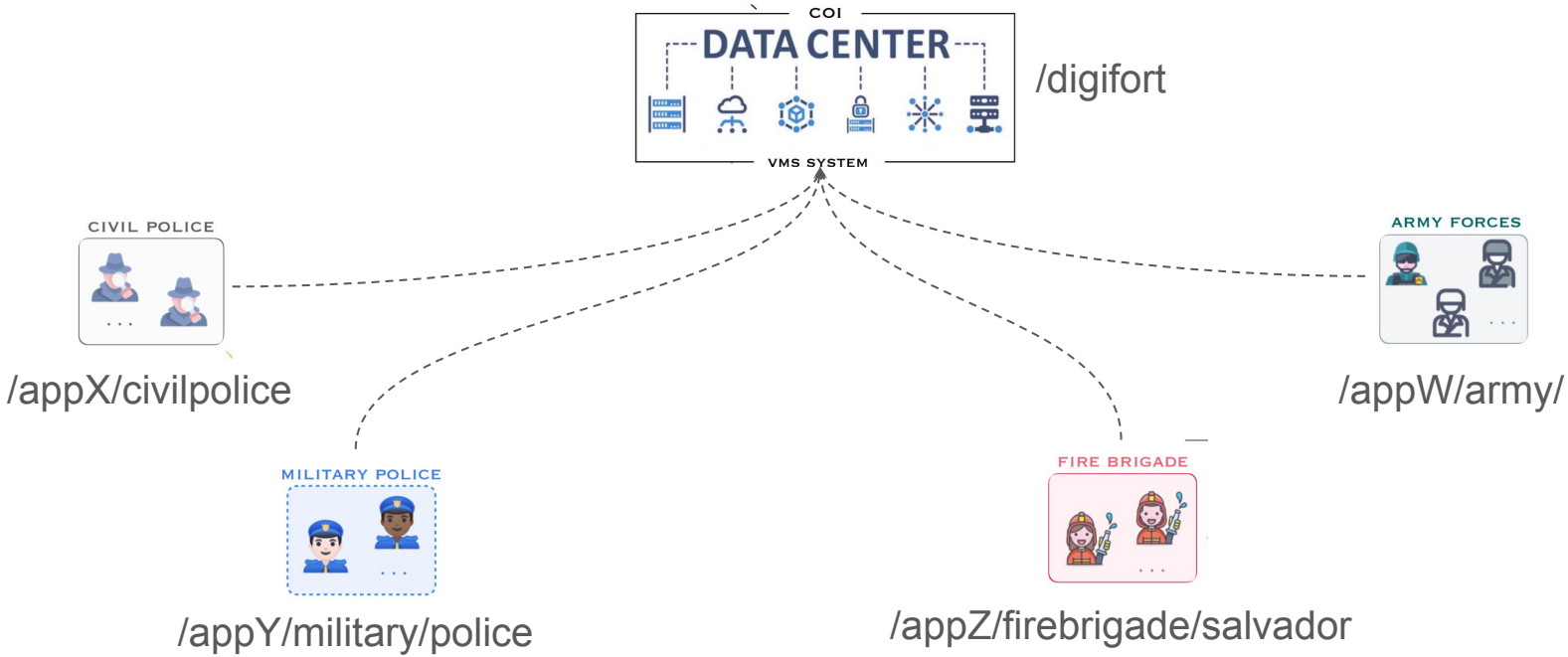
# Surveillance system

The operation and Intelligence Center receive data from different sources to investigate security incidents in real-time and support officers decisions on the field.



# Surveillance system through a NDN perspective

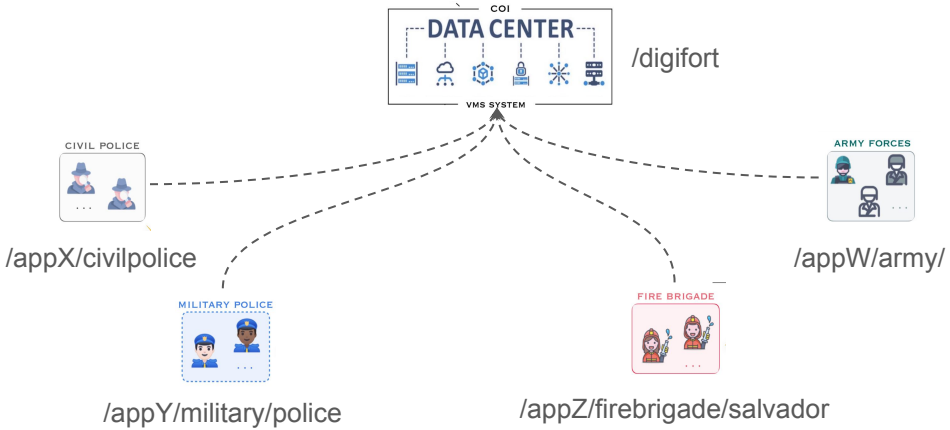
The main security application is centralized and collect data from several other applications from each security institution.



# Security Bootstrapping within a trust zone

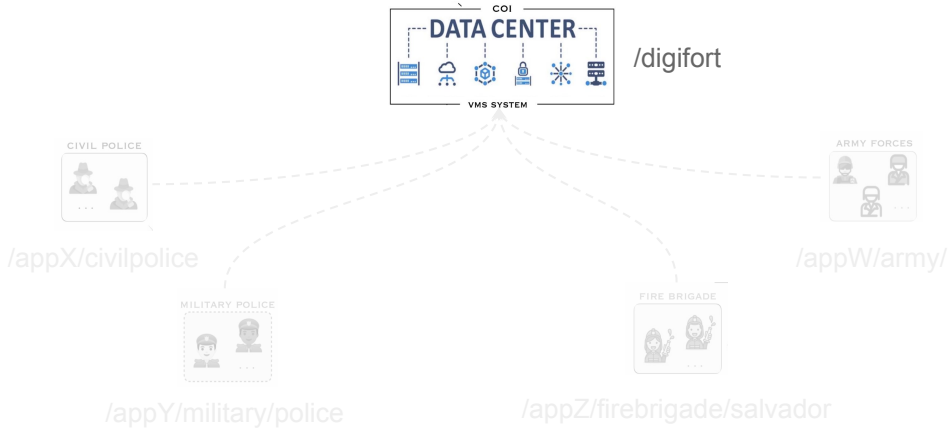
The main security application is centralized and collect data from several other applications from each security institution.

Each application has its own producers and consumers



# Security Bootstrapping within a trust zone

The main security application is centralized and collect data from several other applications from each security institution.




## Each application has its own producers and consumers

All nodes share the same trust anchor

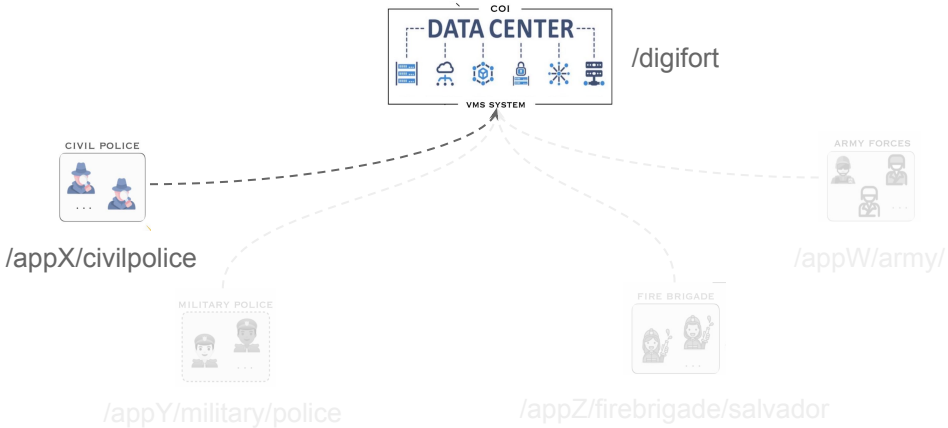
All nodes have installed the trust schema

***Data producing:*** All nodes have an assigned name and can **produce content within the zone**, according to the rules defined in the trust schema

***Data consumption:*** All nodes belonging to the same zone can validate data: i) authenticate the producer; and ii) check the producer legitimacy

# Data consumption involving different trust zones

The main security application is centralized and collect data from several other applications from each security institution.




## The entities in /digifort application must be able to consume data from the other applications

The nodes **HAVE DIFFERENT** trust anchors and trust schemas

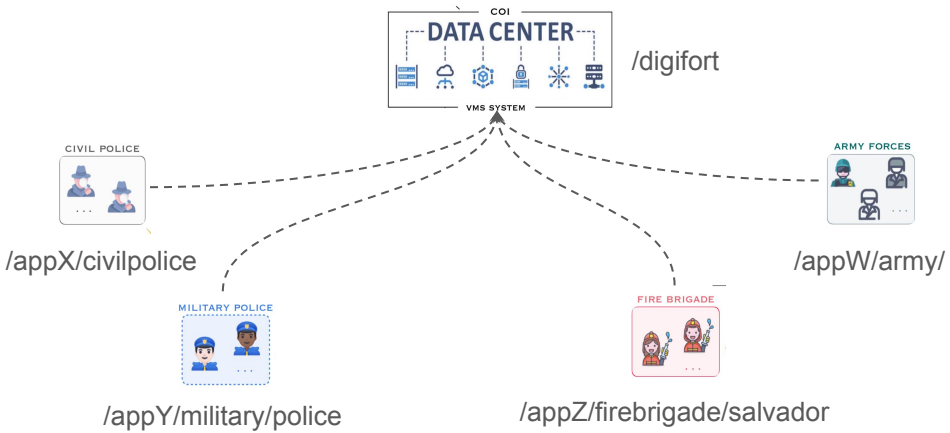
Data consumption:

The entities from digifort **CAN NOT** authenticate the producer from civil police app, because they have different trust anchor

The entities from digifort **CAN NOT** check the producer legitimacy, because they do not have the other zone trust schema

# Establishing Trust Across Different Zones

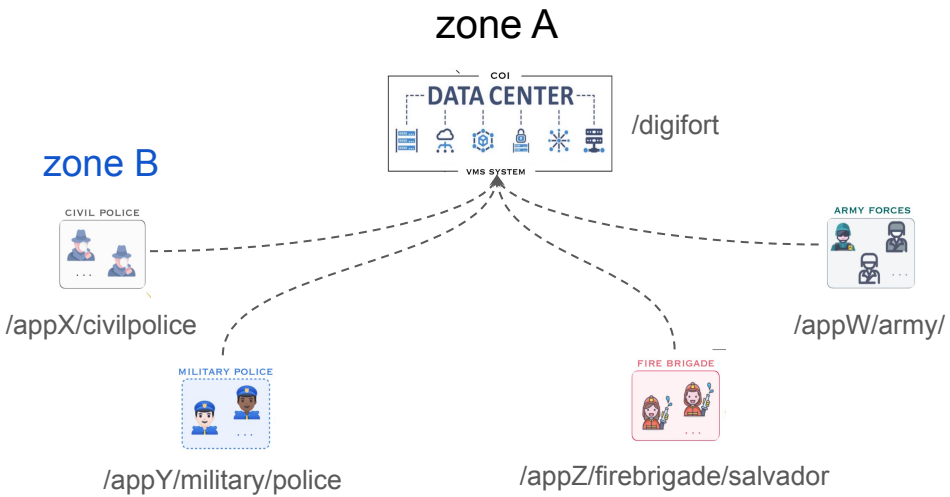
Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?

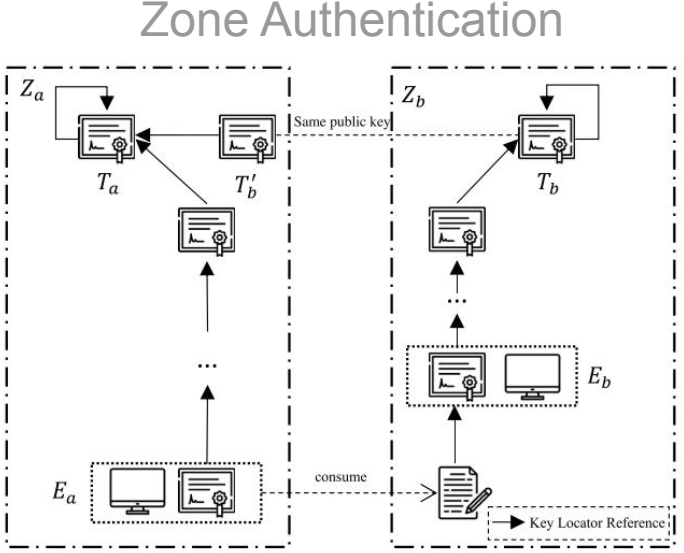



Let's borrow some ideas from Intertrust design…

# Zone authentication

Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?



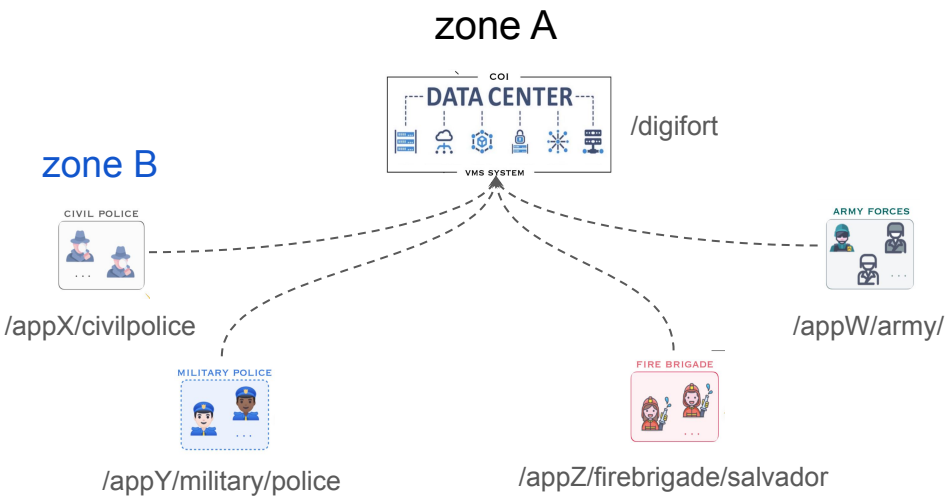




Yu T, Ma X, Xie H, Kocaoğullar Y, Zhang L. Intertrust: establishing inter-zone trust relationships. InProceedings of the 9th ACM Conference on Information-Centric Networking 2022 Sep 6 (pp. 180-182).

Zone $a$ authenticates Zone $b$ by allowing $Tb$ as an external termination point of cryptographic verifications.

# Data consumption and validation across zones

Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?




## After Zone Authentication…

The entities from zone A (digifort) **CAN** authenticate entities from zone B (civil police app), since *Tb'* is the zone B trust anchor signed by zone A trust anchor.

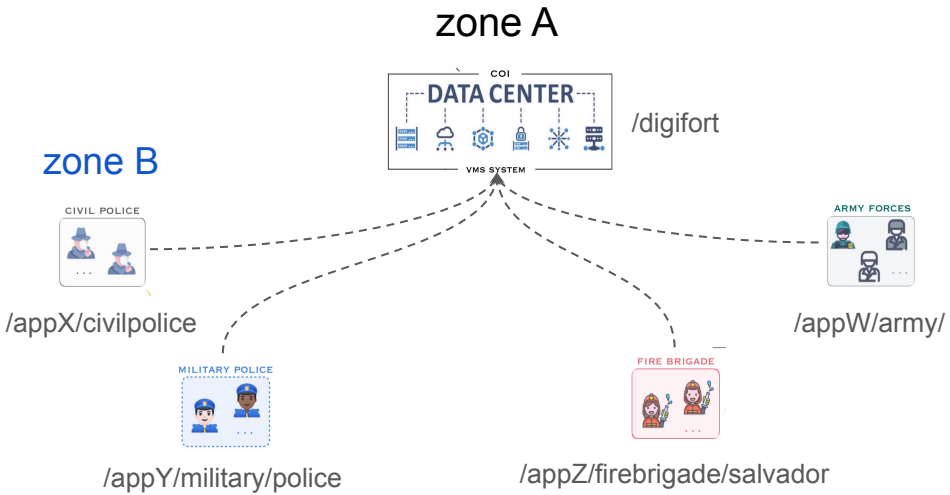
**but**

They still need to verify whether is a legitimate producer in zone A's trust model.

All entities in *Z*one $b$ are authenticated by *Z*one $a$ after Zone Authentication, as all the verification chains of their data packets terminate at $Tb$.

# Learning trust policies

Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?




## Zone Authorization?

**/digifort trust schema**

```
rule 1{},
rule 2{},
rule 3{},

...

trust-anchor
{
  type file
  file-name "digifort.cert"
}
```

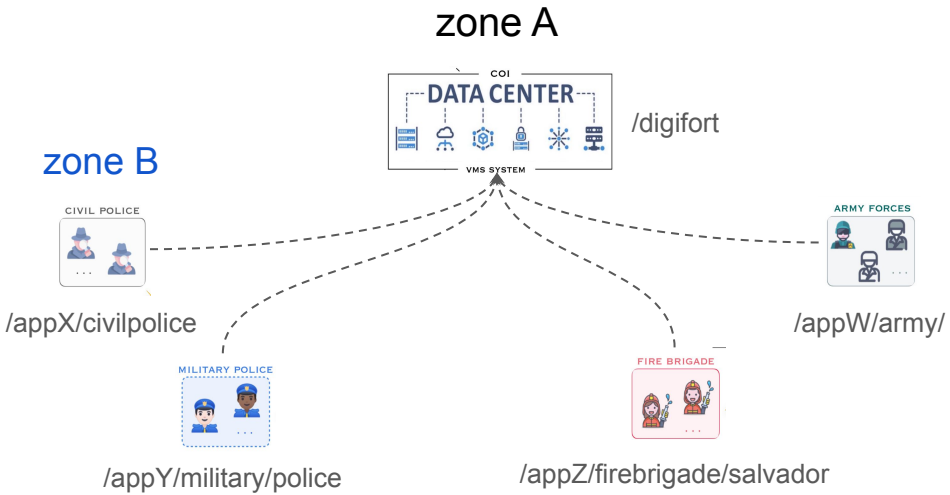
**/appX/civilpolice trust schema**

```
rule 1{},
rule 2{},
rule 3{},

...

trust anchor
{
type file
file-name "appX.cert"
}
```

Zone $a$ needs to define trust rules on the data produced by $Zb$ entities can be validated

# Challenges and Design Considerations

Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?




## Zone Authorization?

The entities from zone A (digifort) **CAN** check the producer legitimacy, because they have the other zone trust schema information

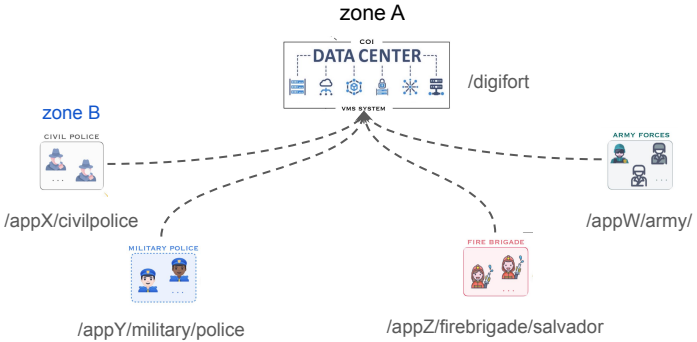
However, **changes in zone B trust schema will trigger changes in zone A trust schema**

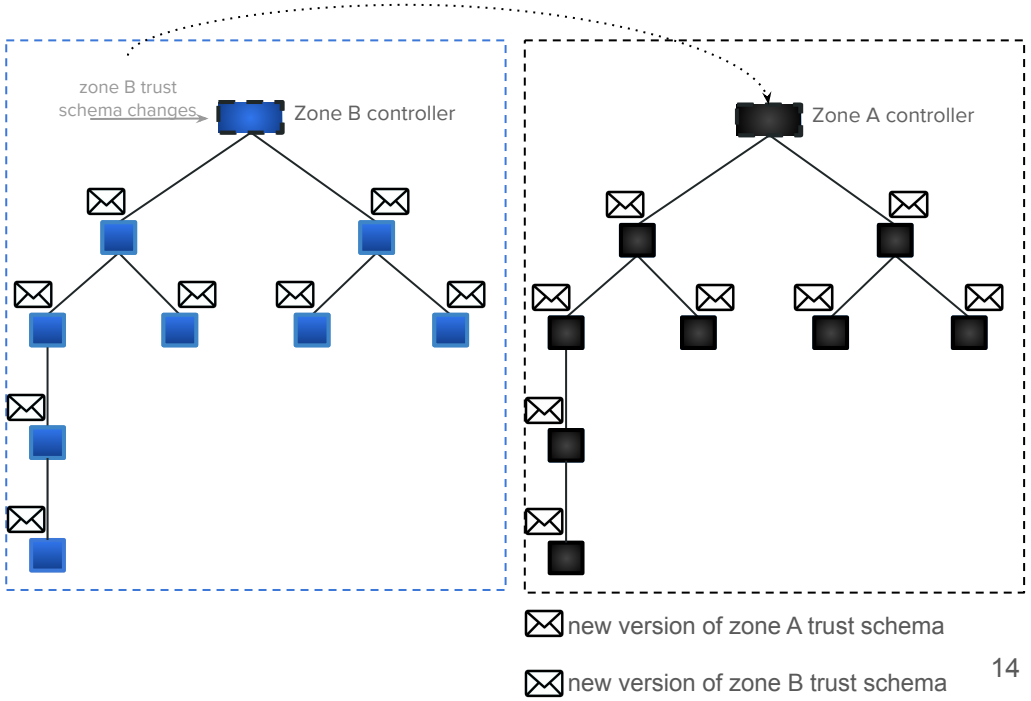
**/digifort trust schema**

```
rule 1{},
rule 2{},
rule 3{},
...
trust-anchor? {
type file
file-name "appX.cert"
}
rule 1{},
rule 2{},
rule 3{},
...
{
trust-anchor
{
  type file
  file-name "digifort.cert"
}
```

# Challenges and Design Considerations

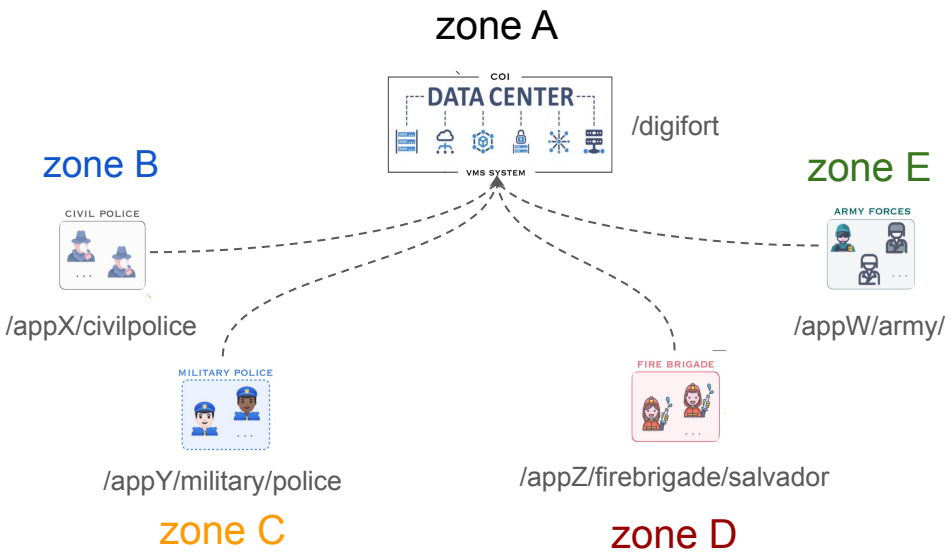
Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?



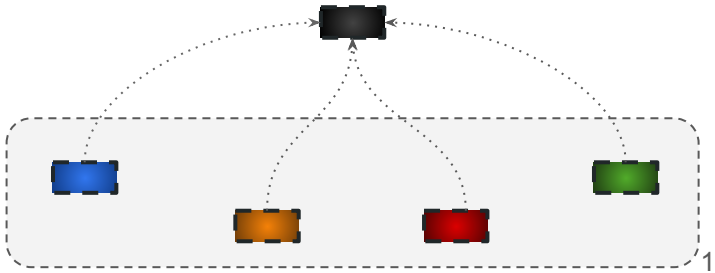
# Challenges and Design Considerations

Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?



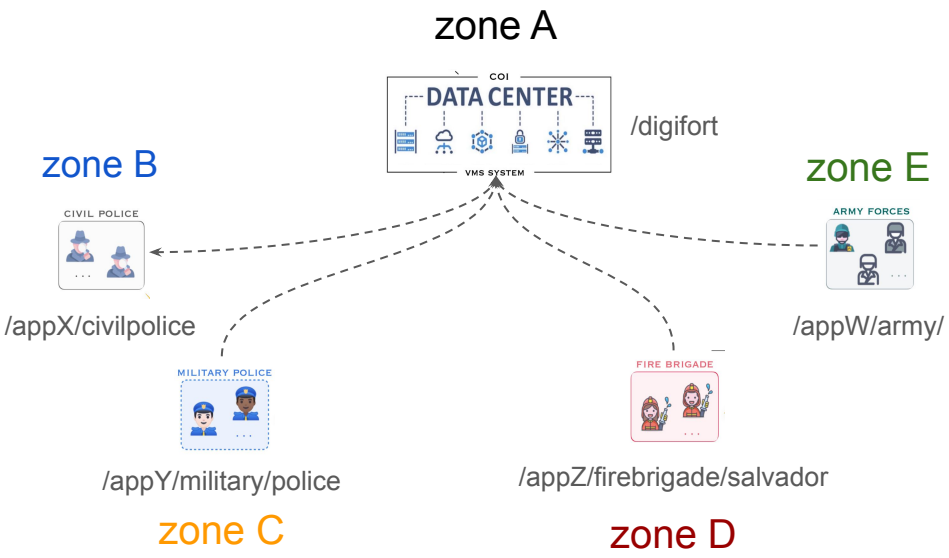

The problem escalates…

every time an authenticated zone changes its trust schema, zone A must update its own trust schema



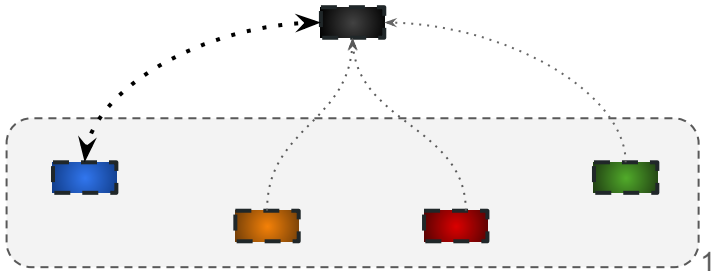
# Challenges and Design Considerations

Considering that each application is a different trust zone, how can entities in zone A (e.g. digifort app) consume and validate data that was produced by entities in zone B (e.g. Civil Police)?




Another design consideration…

Trust relations can be unidirectional or bidirectional (e.g. zone A needs to consume data from zone B, and vice versa)



# Summary of the questions and design considerations

- What is the best way to learn zone B trust rules in zone A?
- How can we deal with trust schemas synchronization from several zones?
- What is the best way to learn trust policies in a bidirectional trust relation?

# Q/A
# Thanks!

leobino@ufba.br