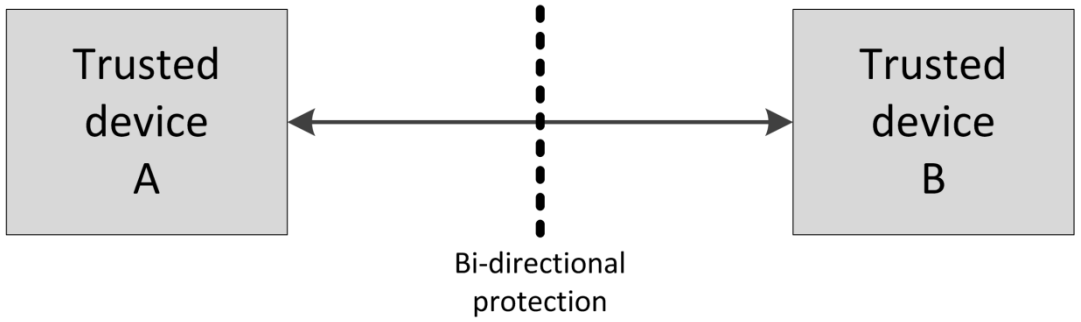
How ISO 21217 works

Please view as a “Slide Show”

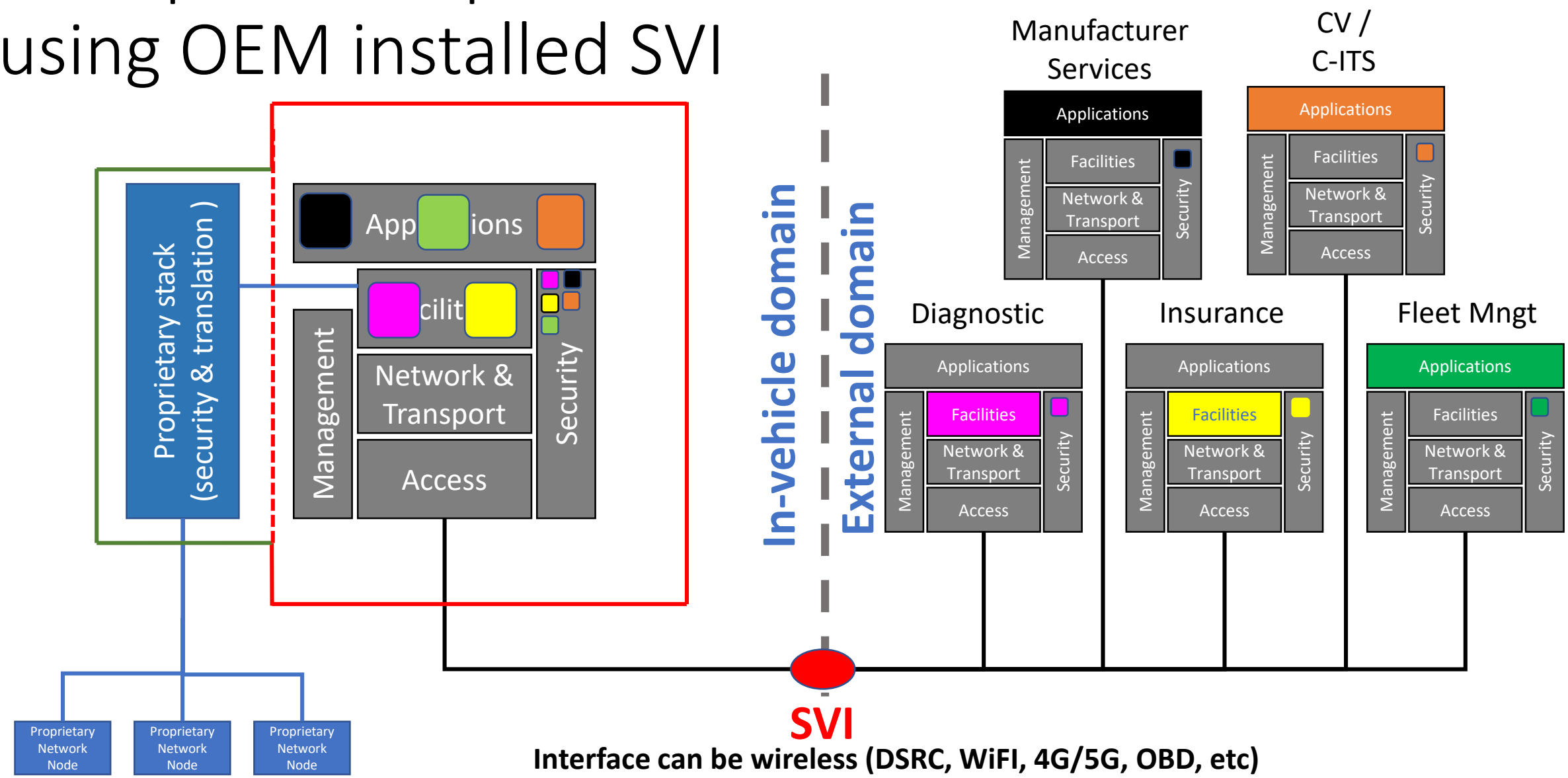
CEN PT1605

The basic situation

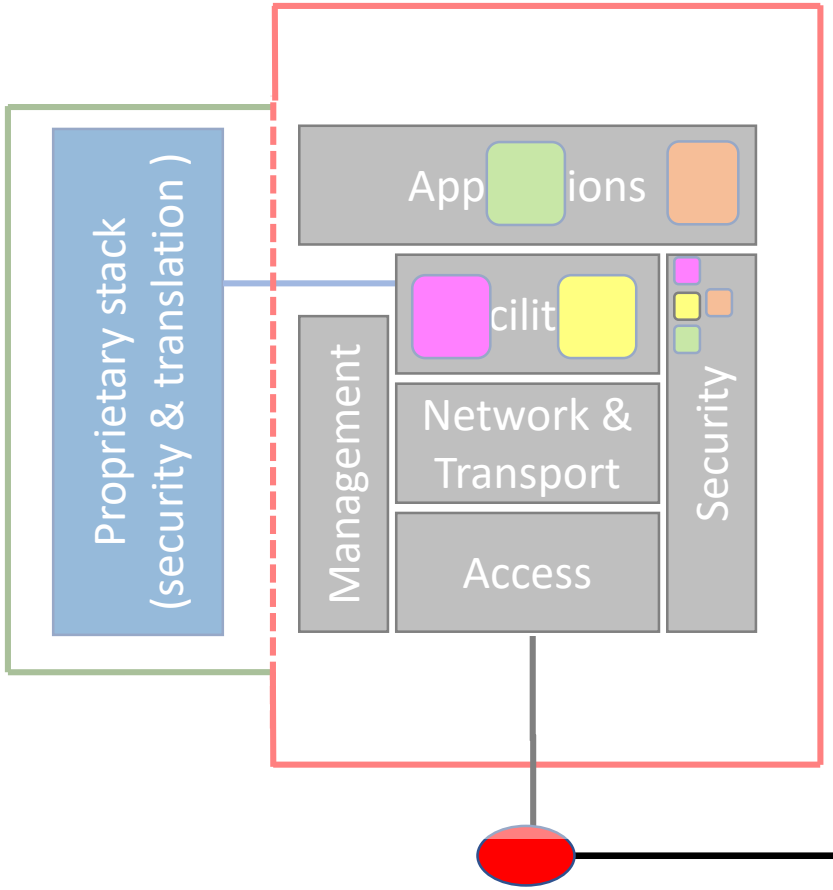
- Two devices cooperate in a trusted way, i.e. exchange information in secure application sessions.

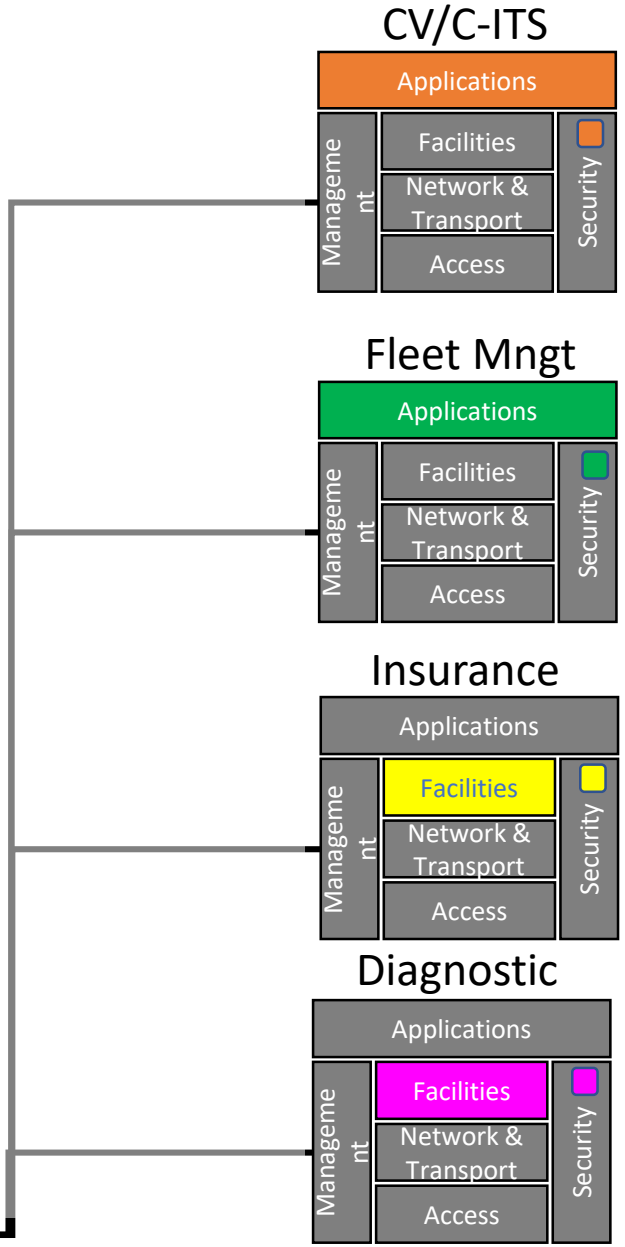


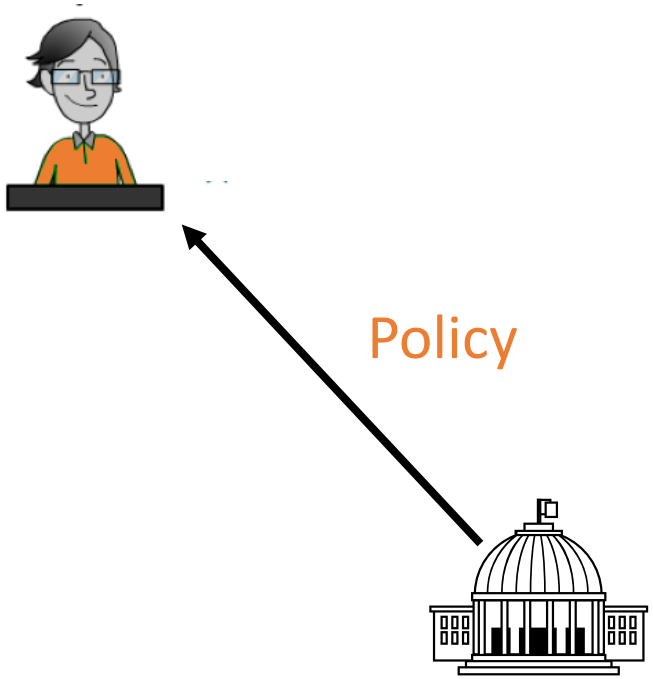
Example: Multiple after-market services using OEM installed SVI



Security: Authentication / Authorization

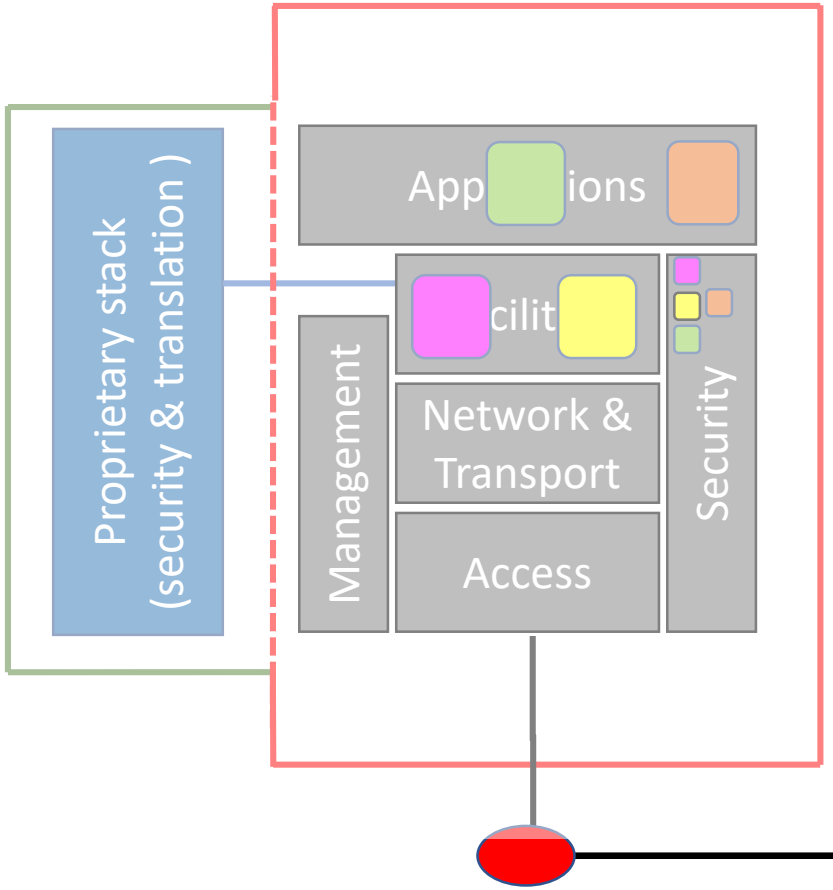


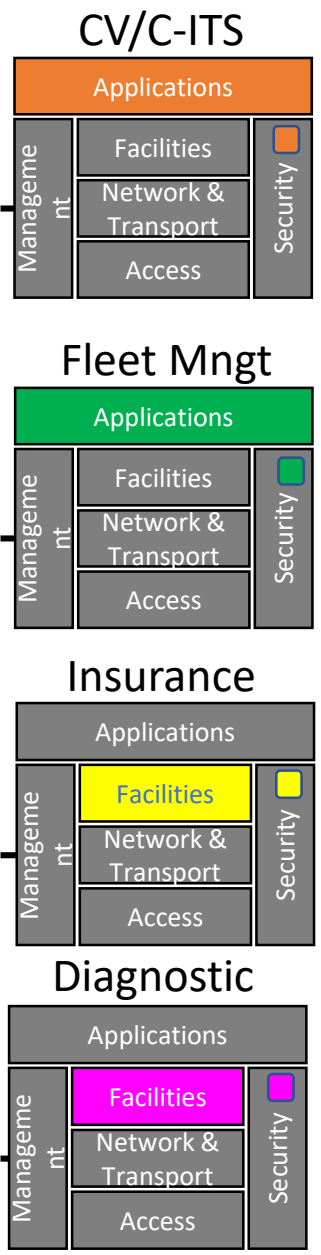




autocare™ ASSOCIATION
Independence drives us.

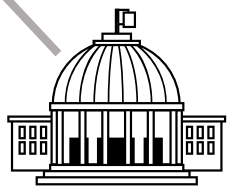
Security: Authentication / Authorization





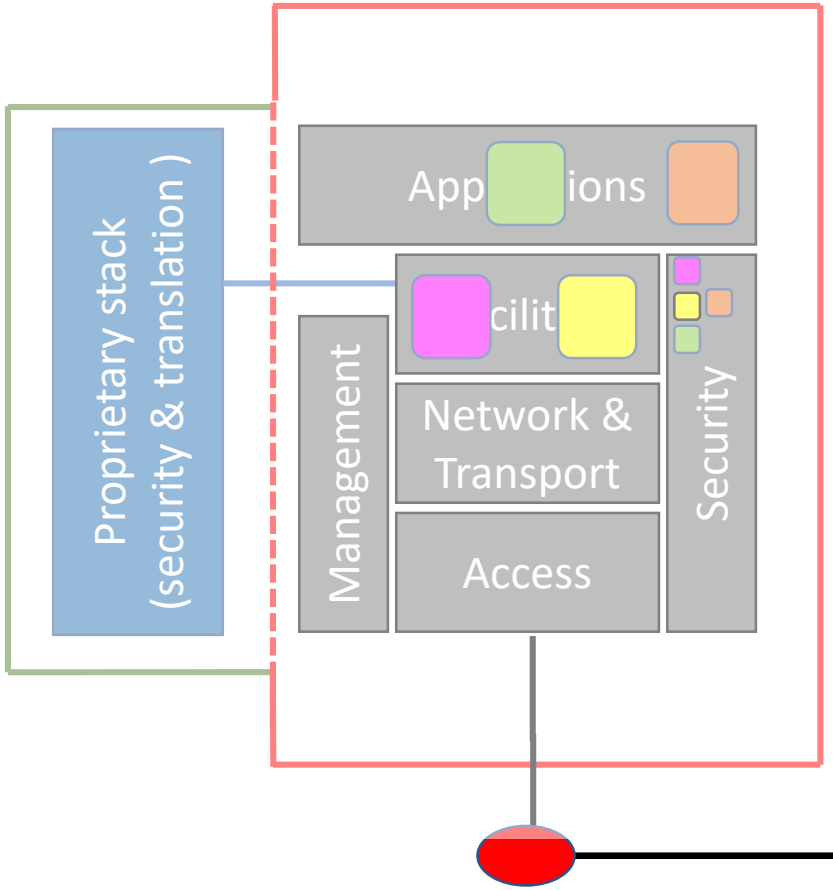
Proof: valid C-ITS Application

Policy

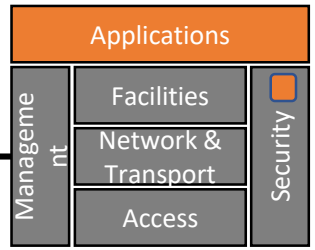


autocare™
ASSOCIATION
Independence drives us.

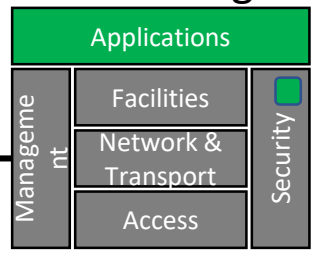
Security: Authentication / Authorization



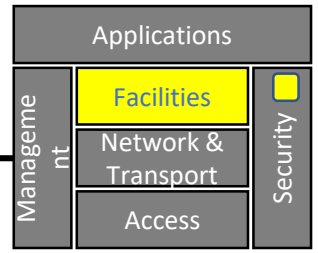
CV/C-ITS



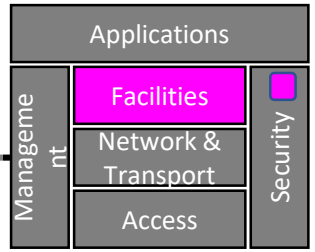
Fleet Mngt



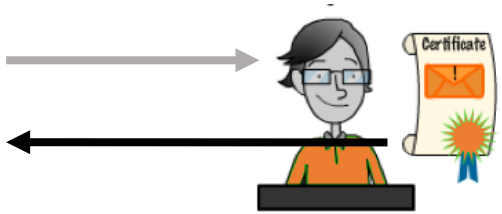
Insurance



Diagnostic

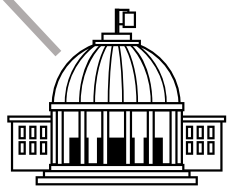


Proof: valid C-ITS Application



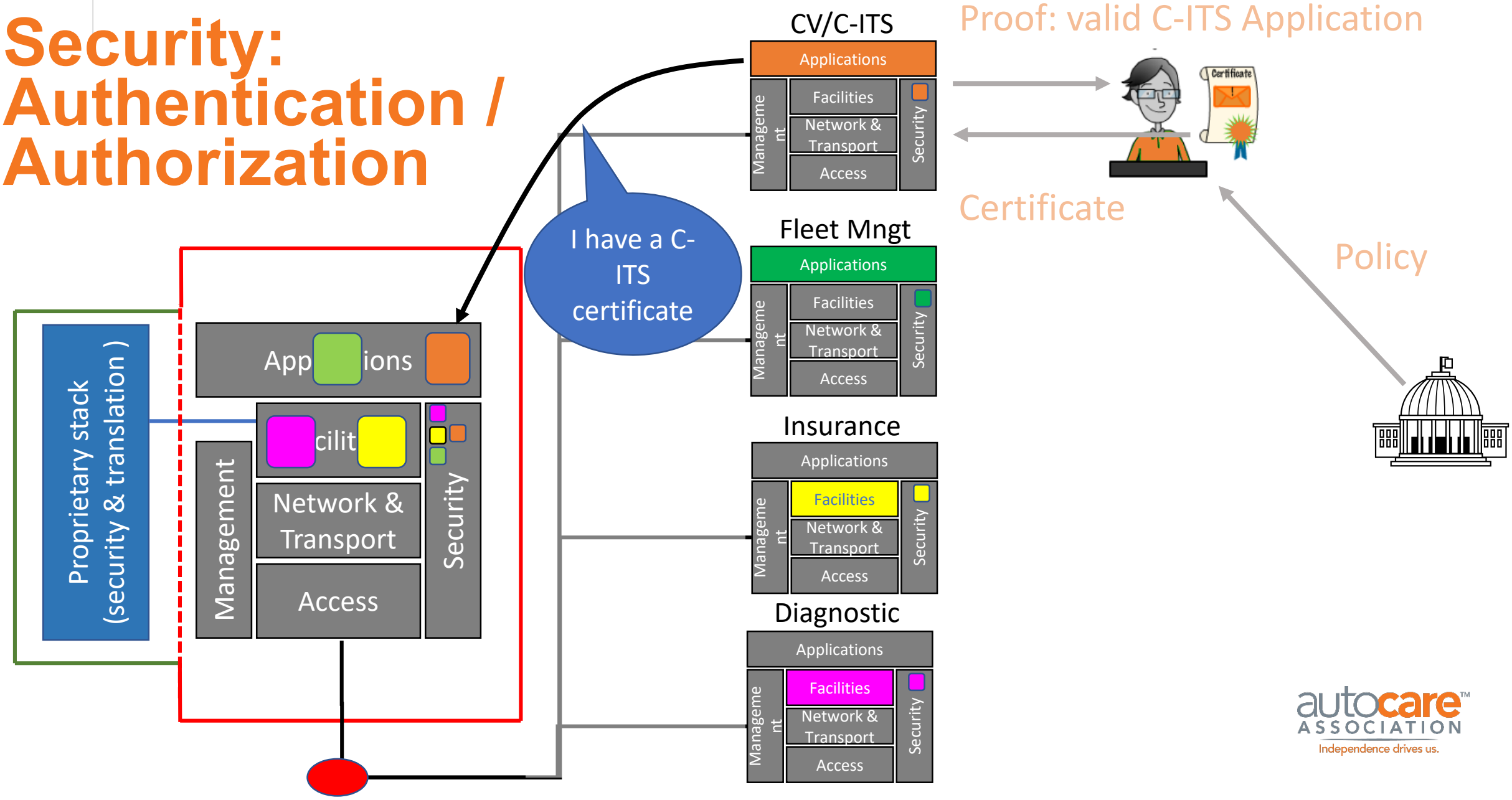
Certificate

Policy



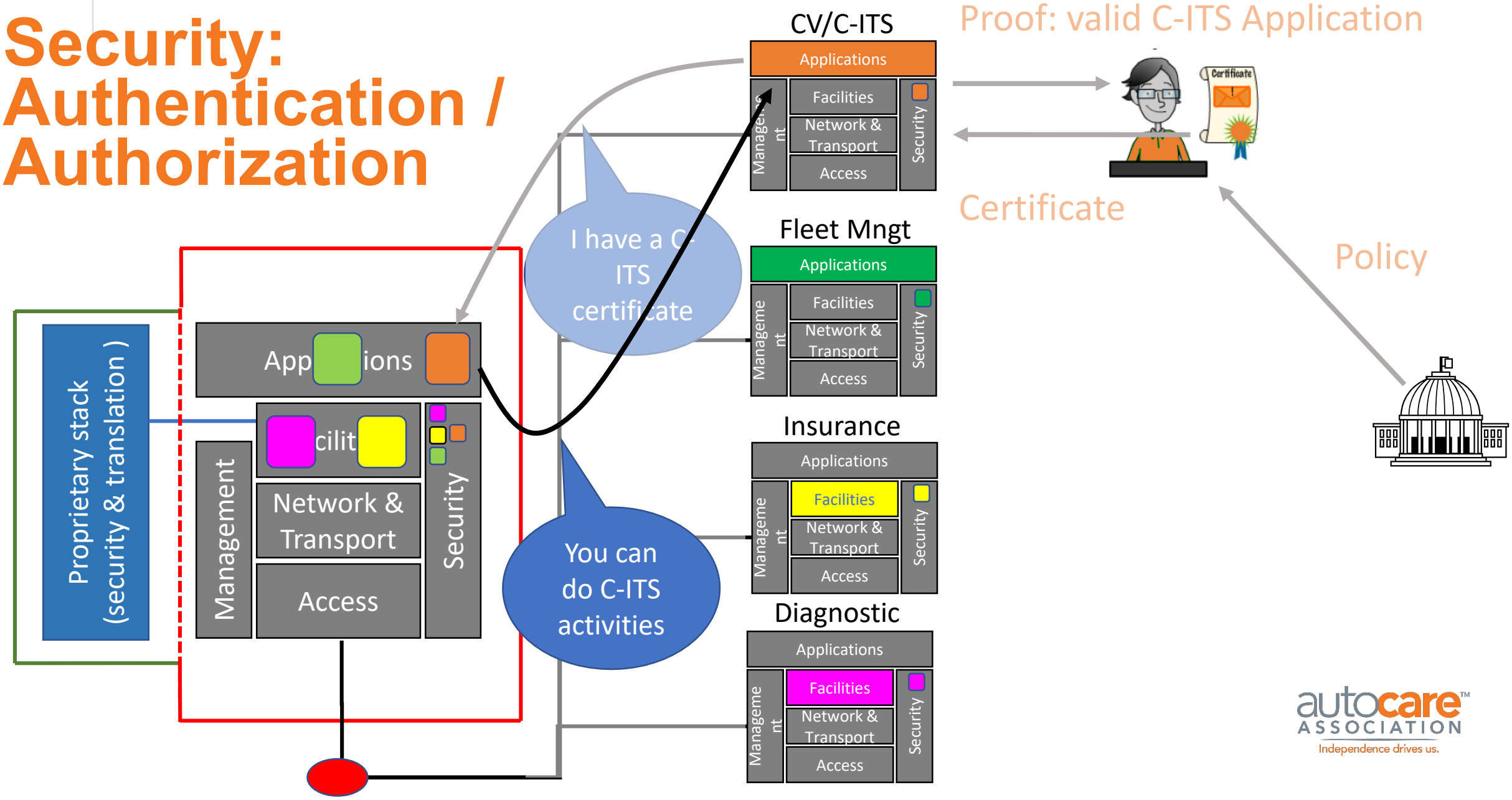
autocare™ ASSOCIATION
Independence drives us.

Security: Authentication / Authorization



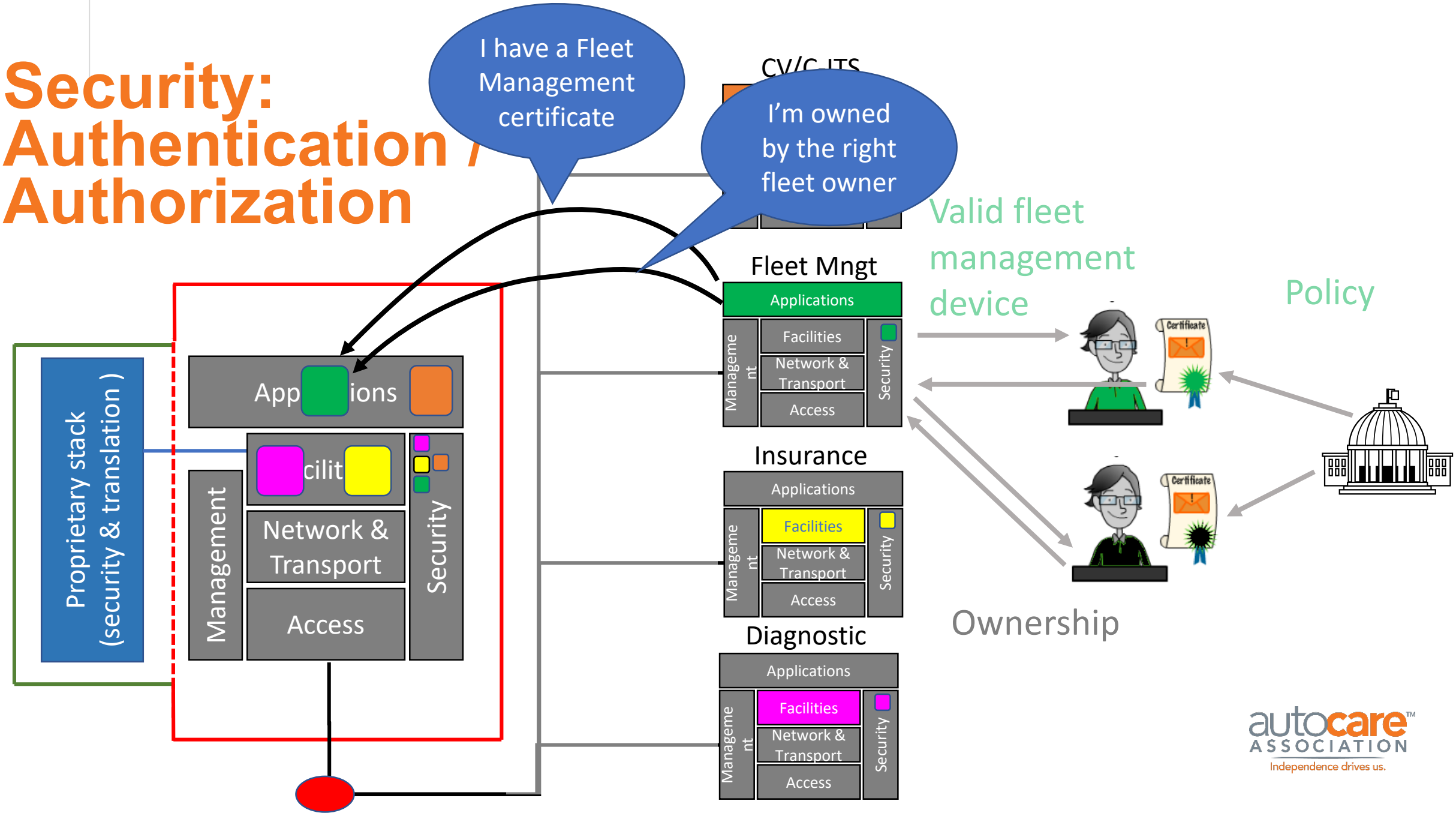
autocare ASSOCIATION
Independence drives us.

Security: Authentication / Authorization



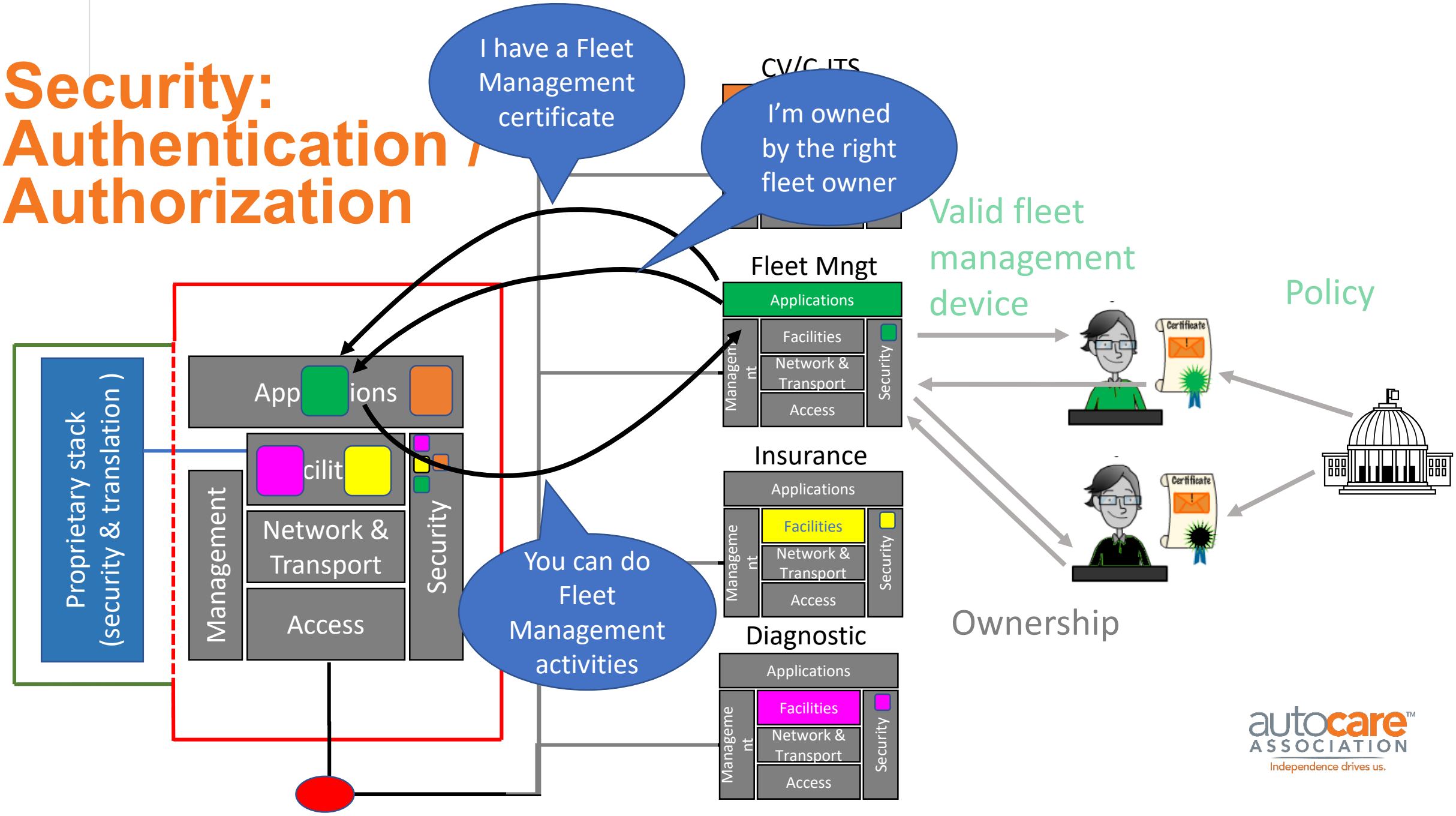
autocare ASSOCIATION
Independence drives us.

Security: Authentication / Authorization



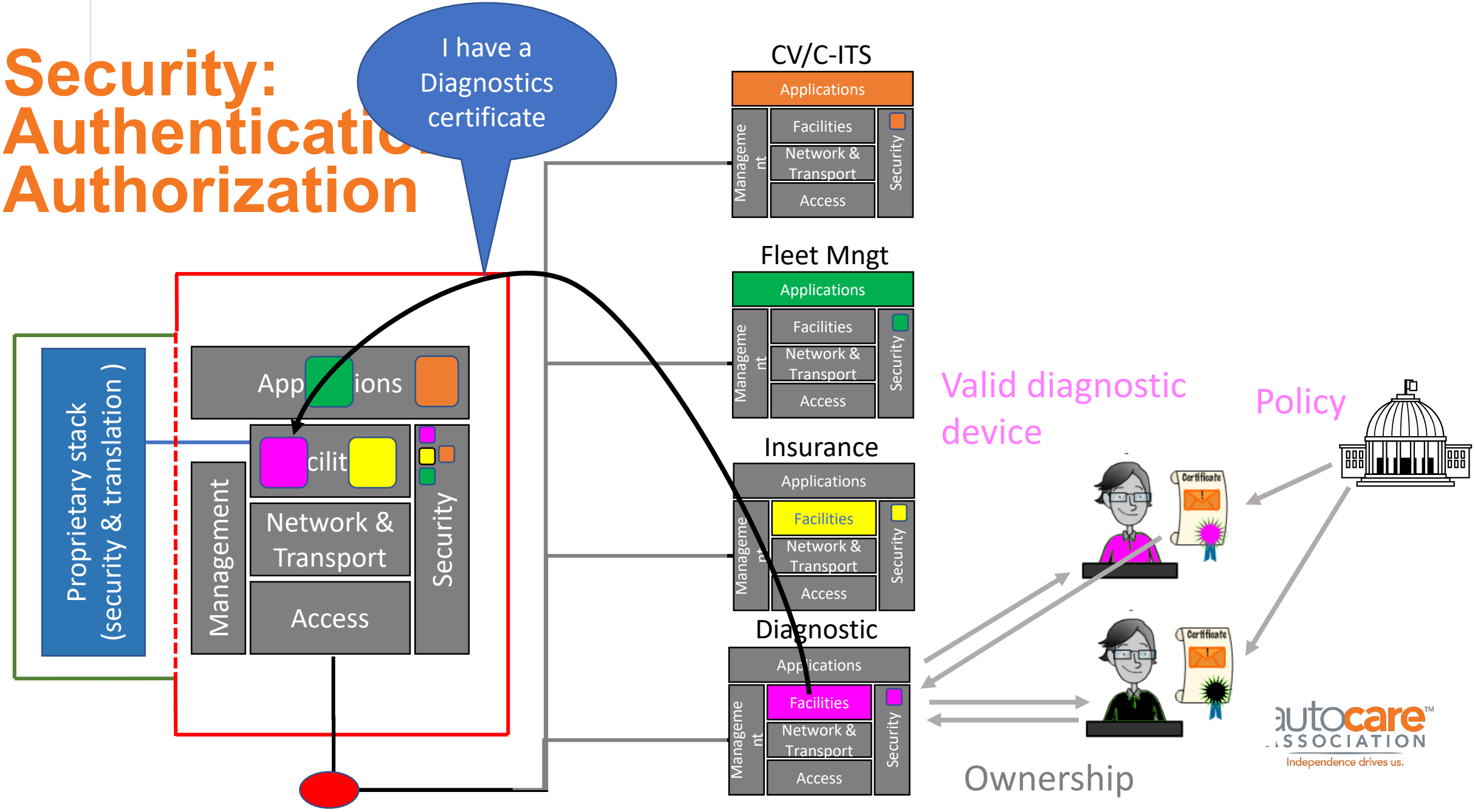
autocare ASSOCIATION
Independence drives us.

Security: Authentication / Authorization

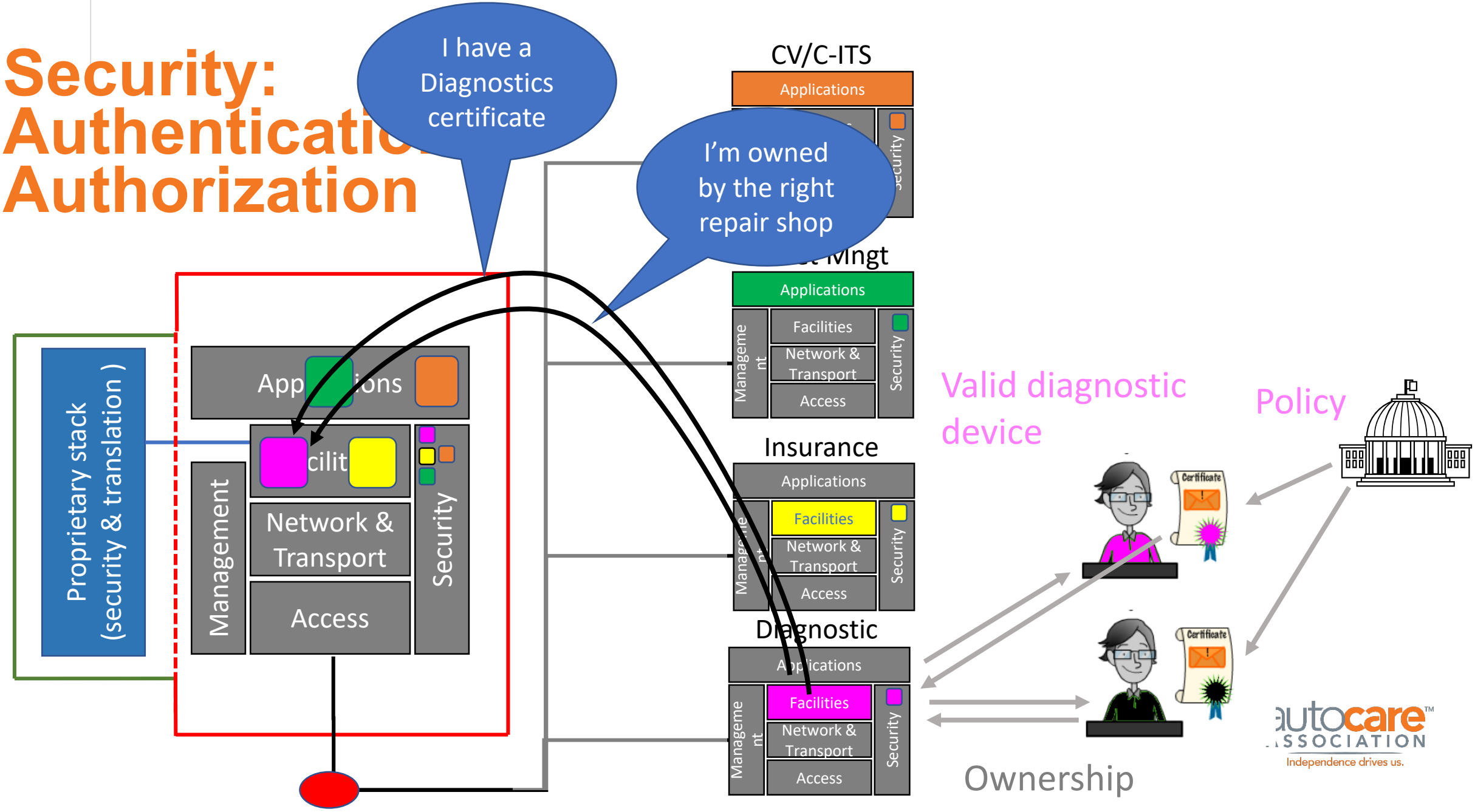


autocare ASSOCIATION
Independence drives us.

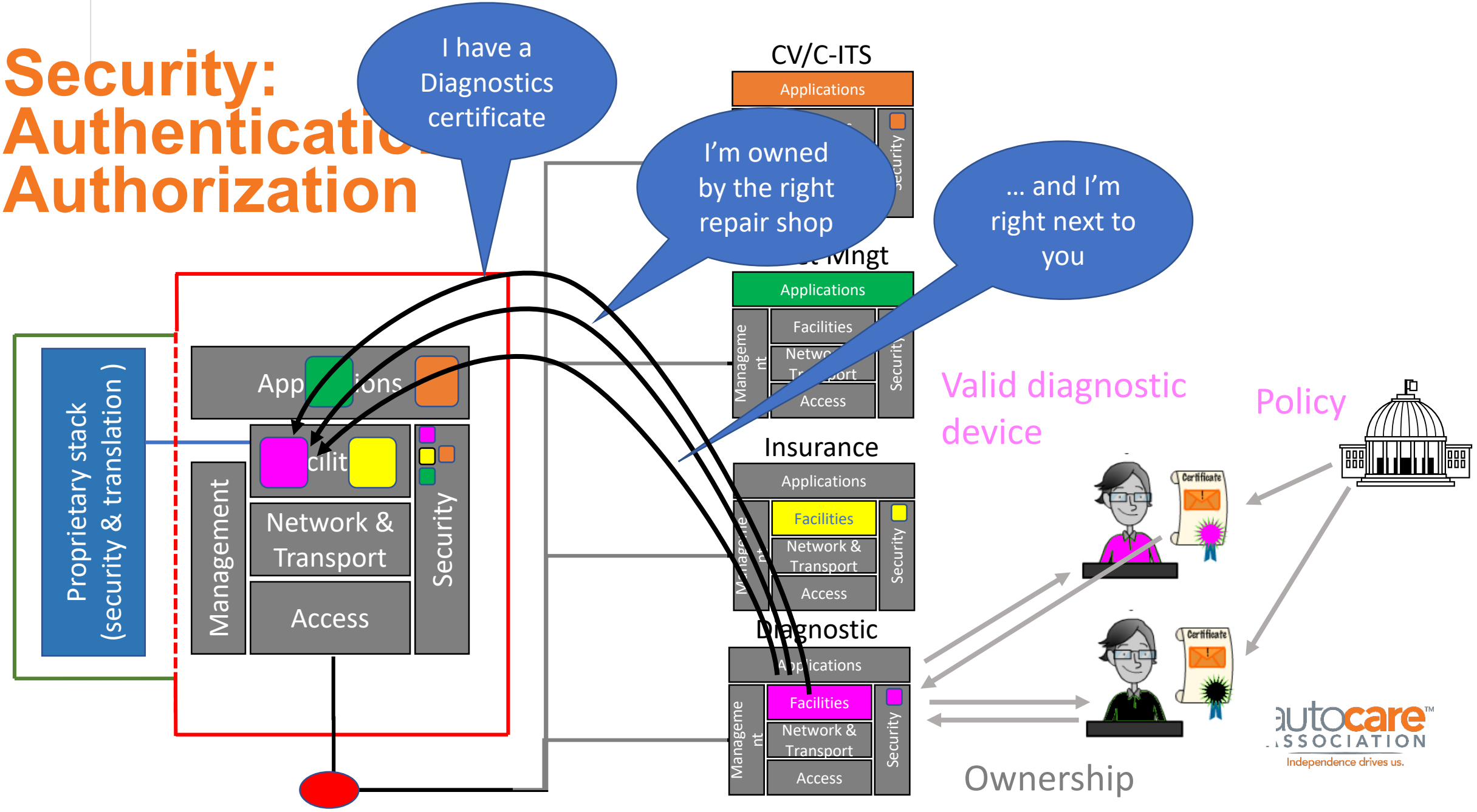
Security: Authentication Authorization



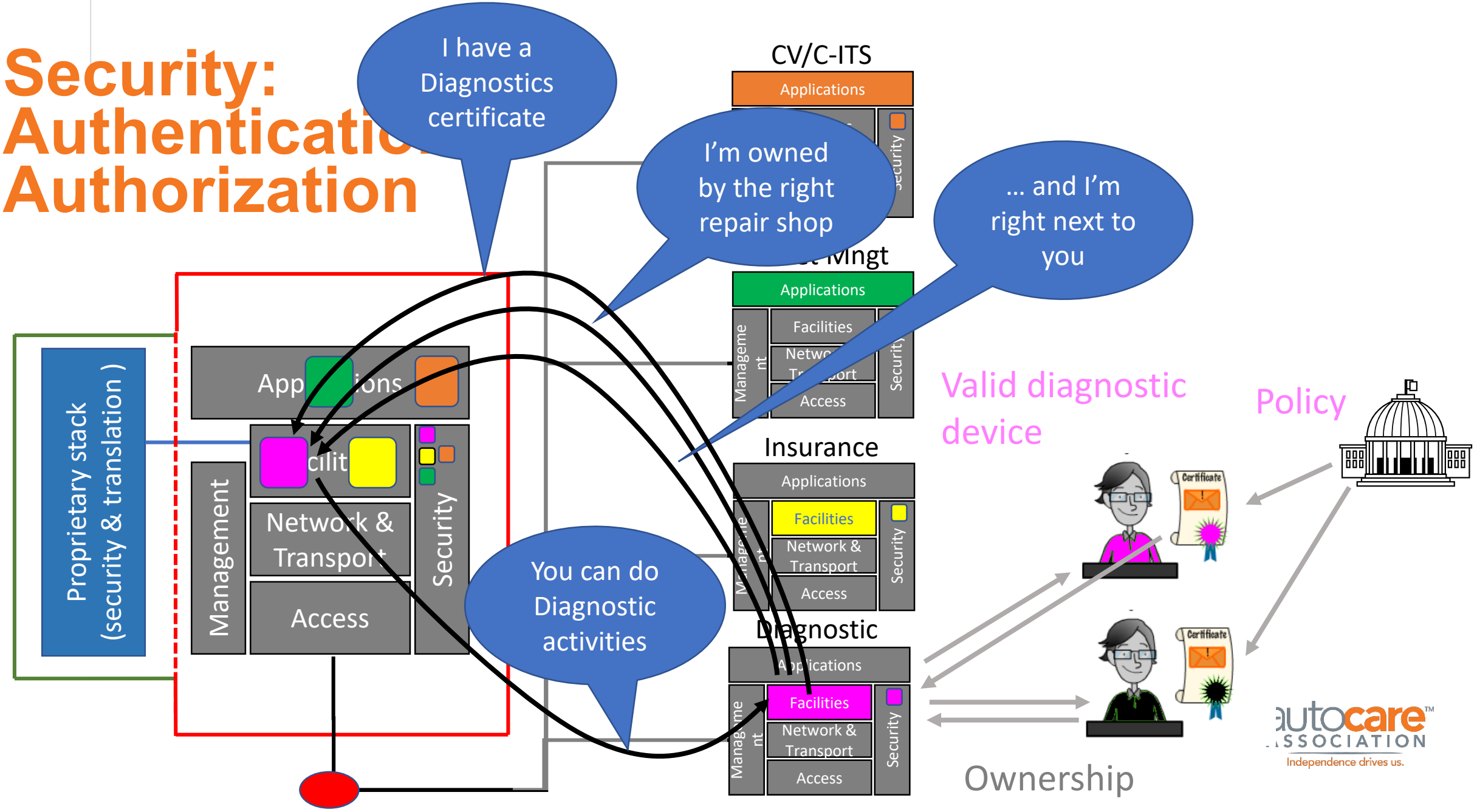
Security: Authentication Authorization



Security: Authentication Authorization

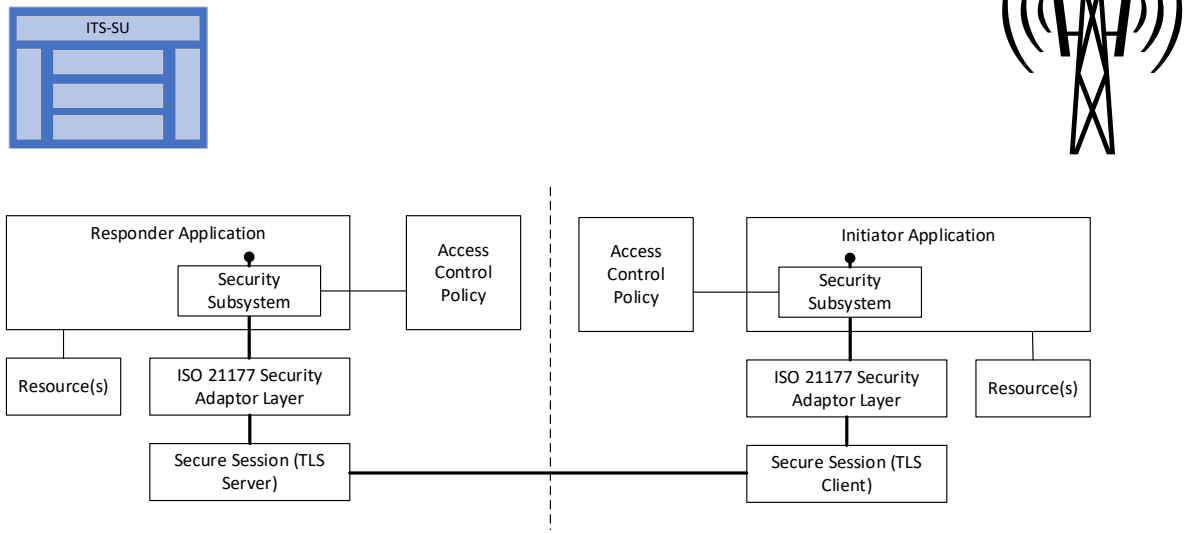


Security: Authentication Authorization

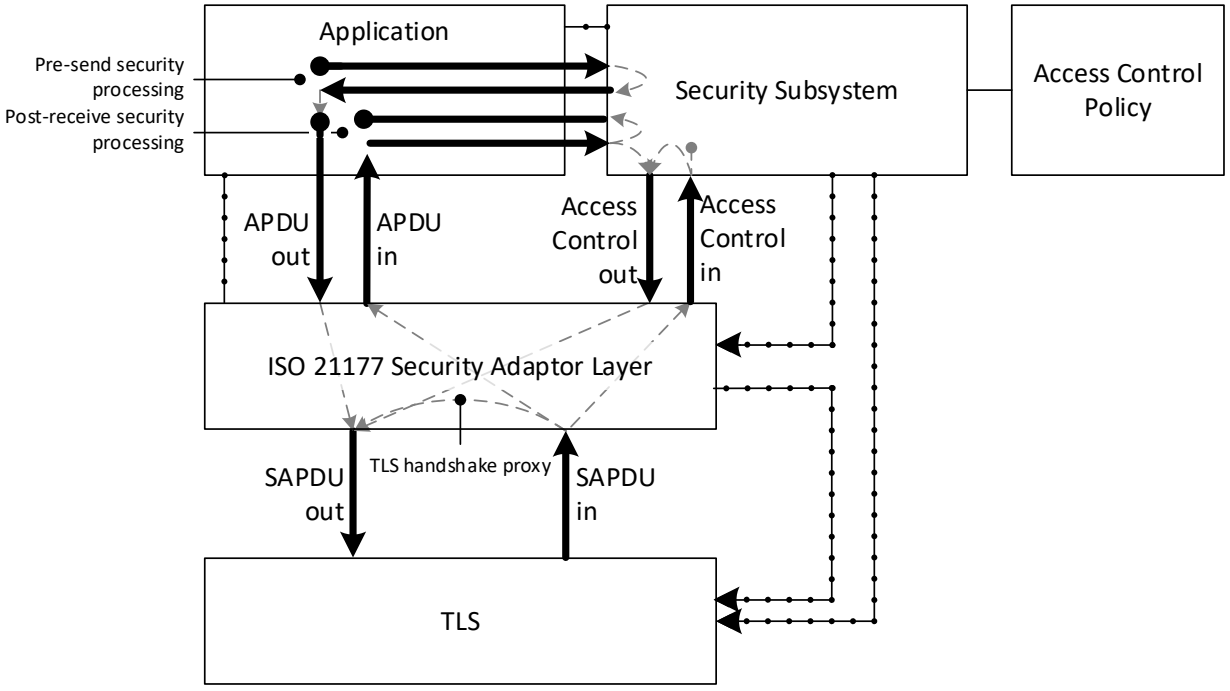


ISO 21177

- Uses internet-standard secure communications protocol, Transport Layer Security (TLS) 1.3
- Enables use of C-ITS (IEEE 1609.2) certificates to directly state permissions
  - More appropriate than identity-based permissions in Mobile Ad Hoc Network (MANET) setting
- Allows each party to present a series of certificates to establish a detailed “authorization state” with the other party
- Becoming adopted by application standards
  - SAE J2945/3 – authenticate / authorize weather reporting applications

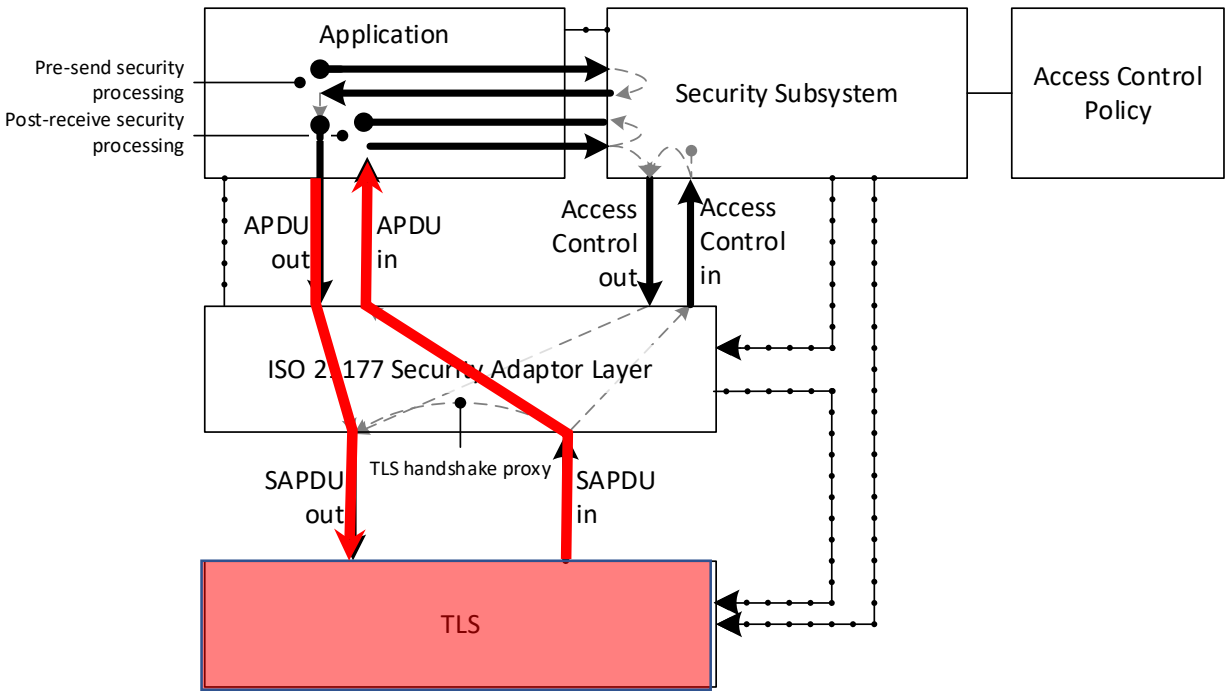


Requirements



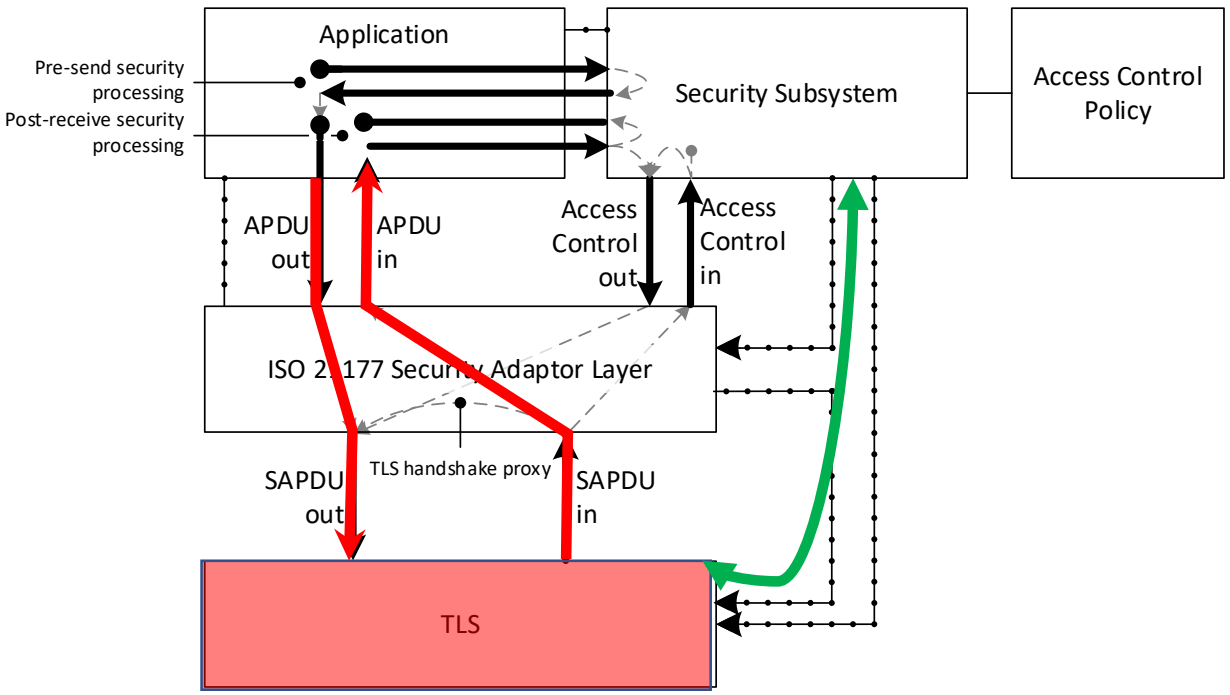
- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting

Requirements



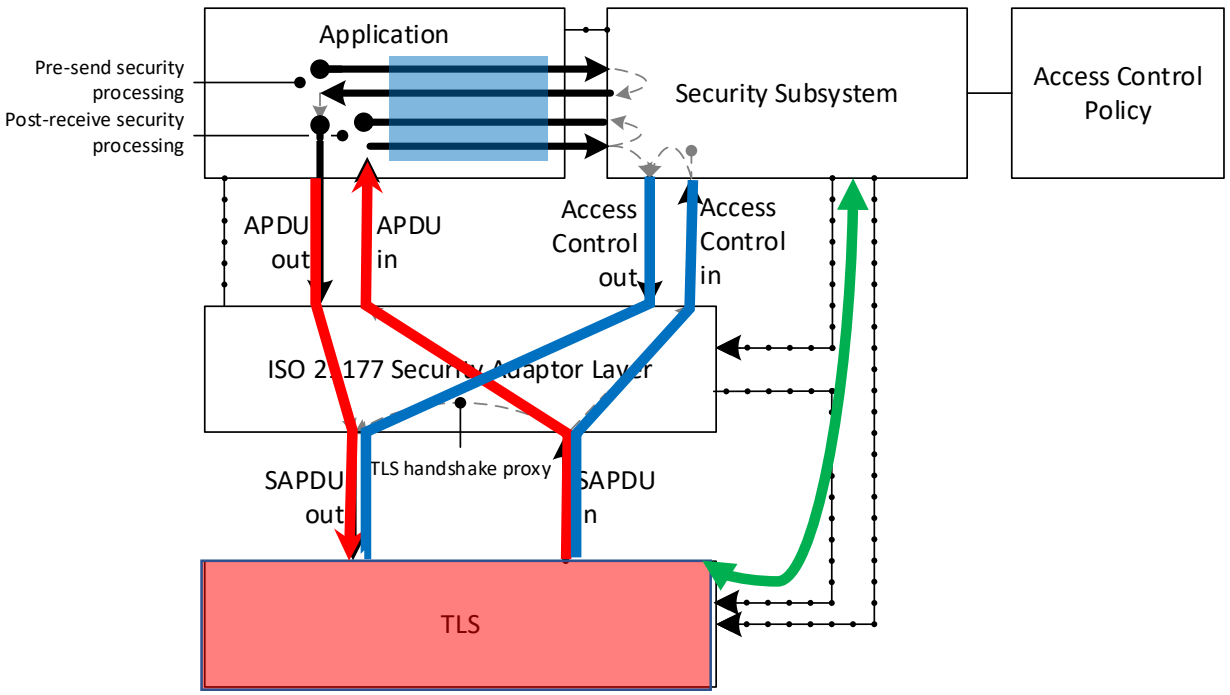
- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting

Requirements



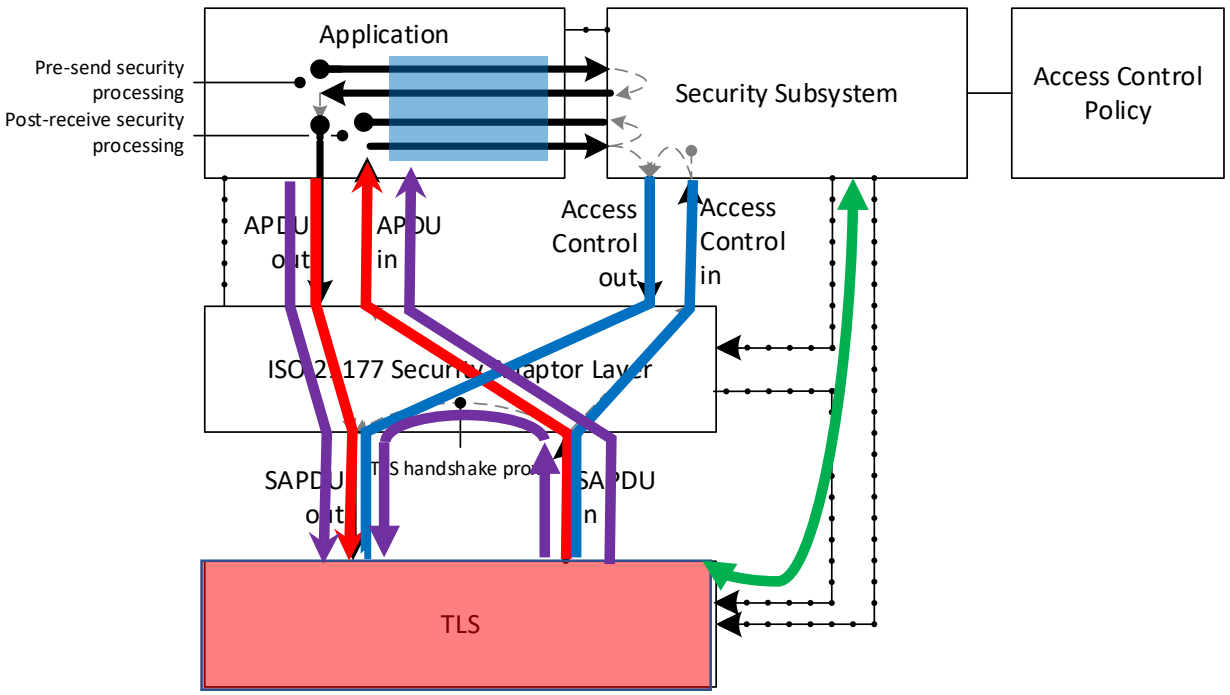
- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting

Requirements



- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting

Requirements



- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting

Security: Authentication / Authorization

- Policy authorities and certificate authorities are already being established to support C-ITS
- This organizational structure can also support authentication and authorization for SVI
- OEMs can enforce reasonable security policies on certificate issuance and freshness
  - OEM security concerns are real and must be taken into account
- However, in this model OEMs are not real-time gatekeepers of access to the information
  - Nevertheless, their security requirements are met