



IoT SAFE

IoT Security Seminar

IoT SAFE – SIM Applet For End-to-End Communications

Jean-Francois Gros

Chair of IoT Security Application Working Group

Trusted Connectivity Alliance



IoT SAFE

Our Membership



Executive:



Full:



Ordinary:





Jean-Francois Gros
Chair of IoT Security Application
Working Group
Trusted Connectivity Alliance

Great teamwork



« Thanks, **Ian**, for directing all this and making it happen »



IoT SAFE

What is IoT SAFE all About?



For the IoT,
security is as important as
connectivity



IoT SAFE

What do we Focus on?

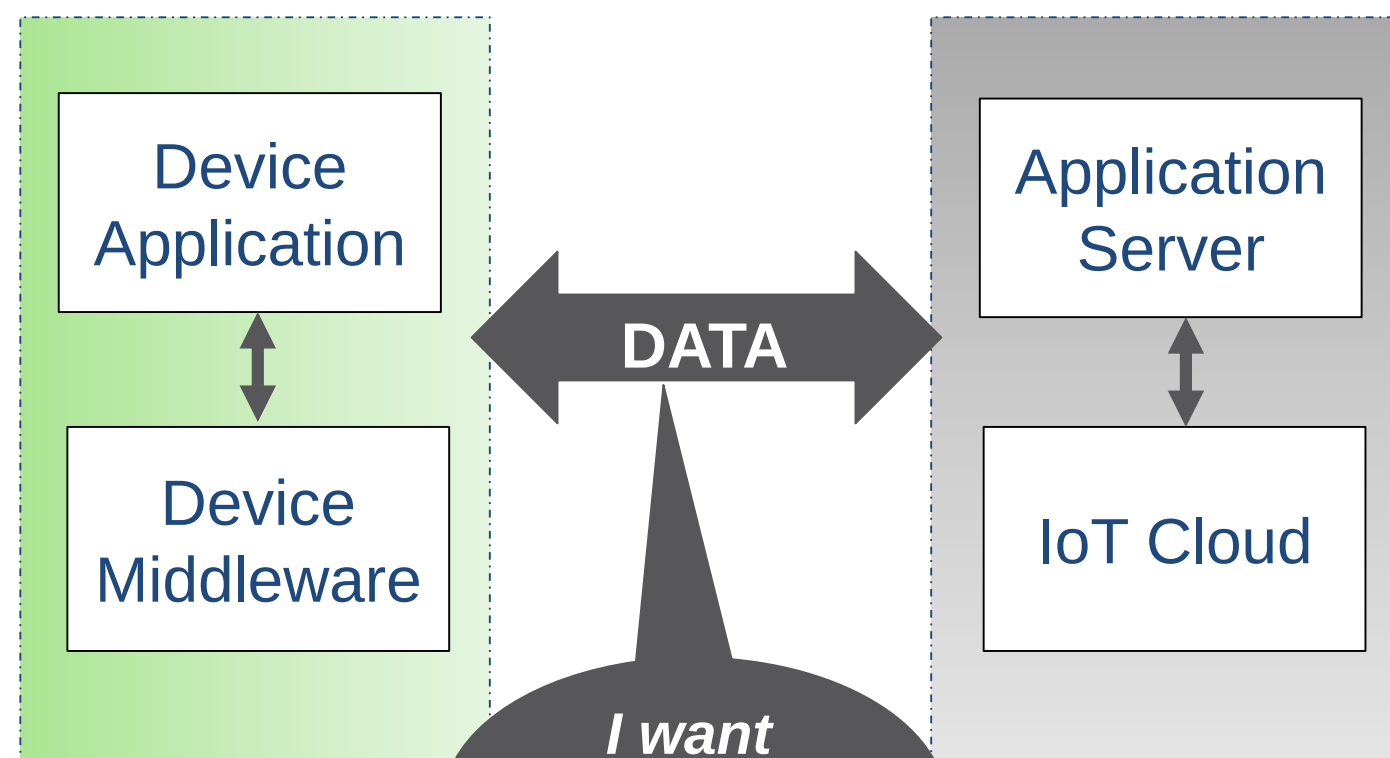
What do we want?

Security: deliver a set of security services to enable specific use cases

First focus: mutual authentication, privacy, integrity

I want to be sure I am sending my data to the right server

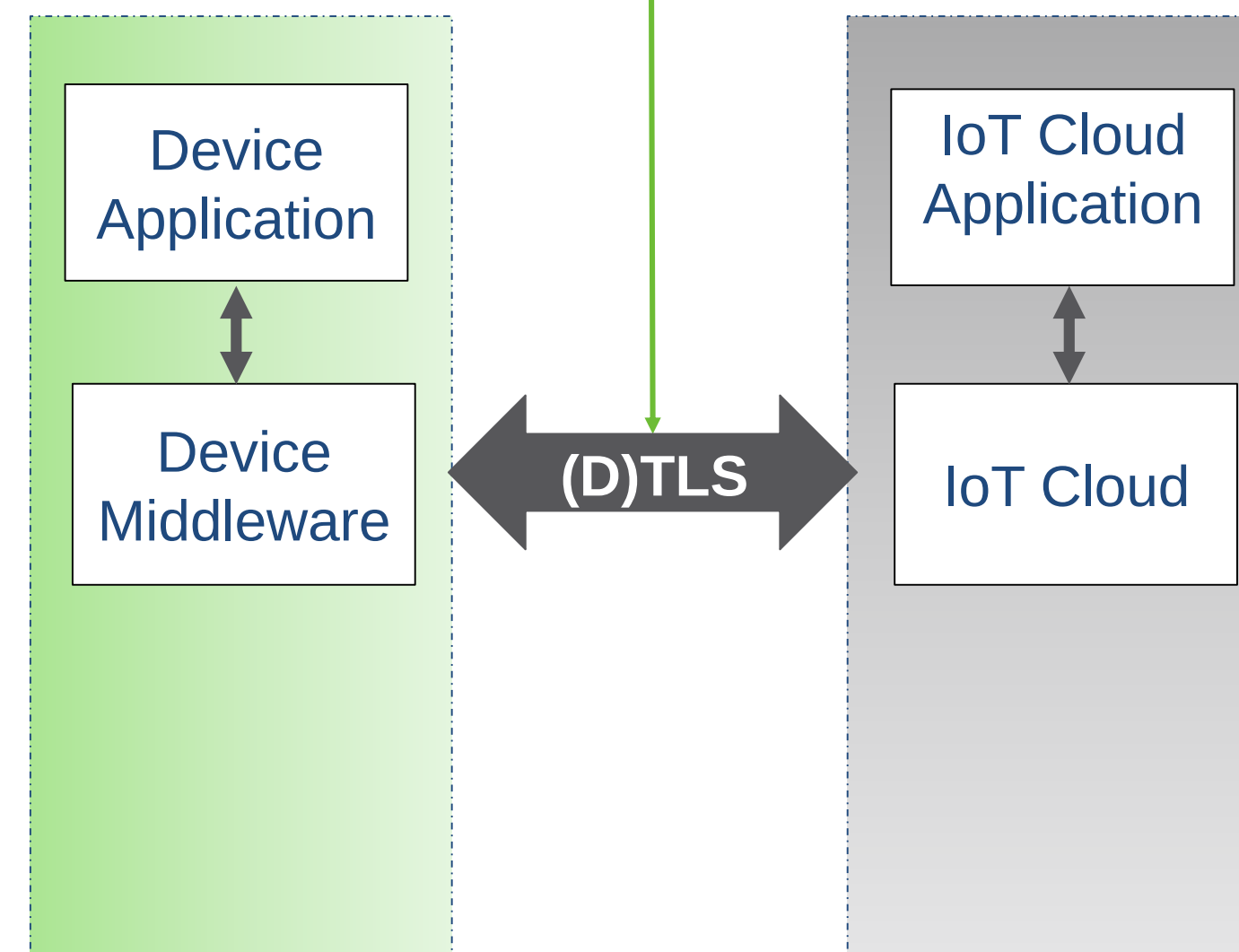
I want to be sure this device is an authorised device



I want confidentiality and integrity

How do we achieve this?

(D)TLS handshake





IoT SAFE

Leverage the Common Denominator Already Present



What do we want?

Security: deliver a set of security services to enable specific use cases

Homogeneity: achieve a solution which can be implemented ubiquitously across all device hardware from all different vendors

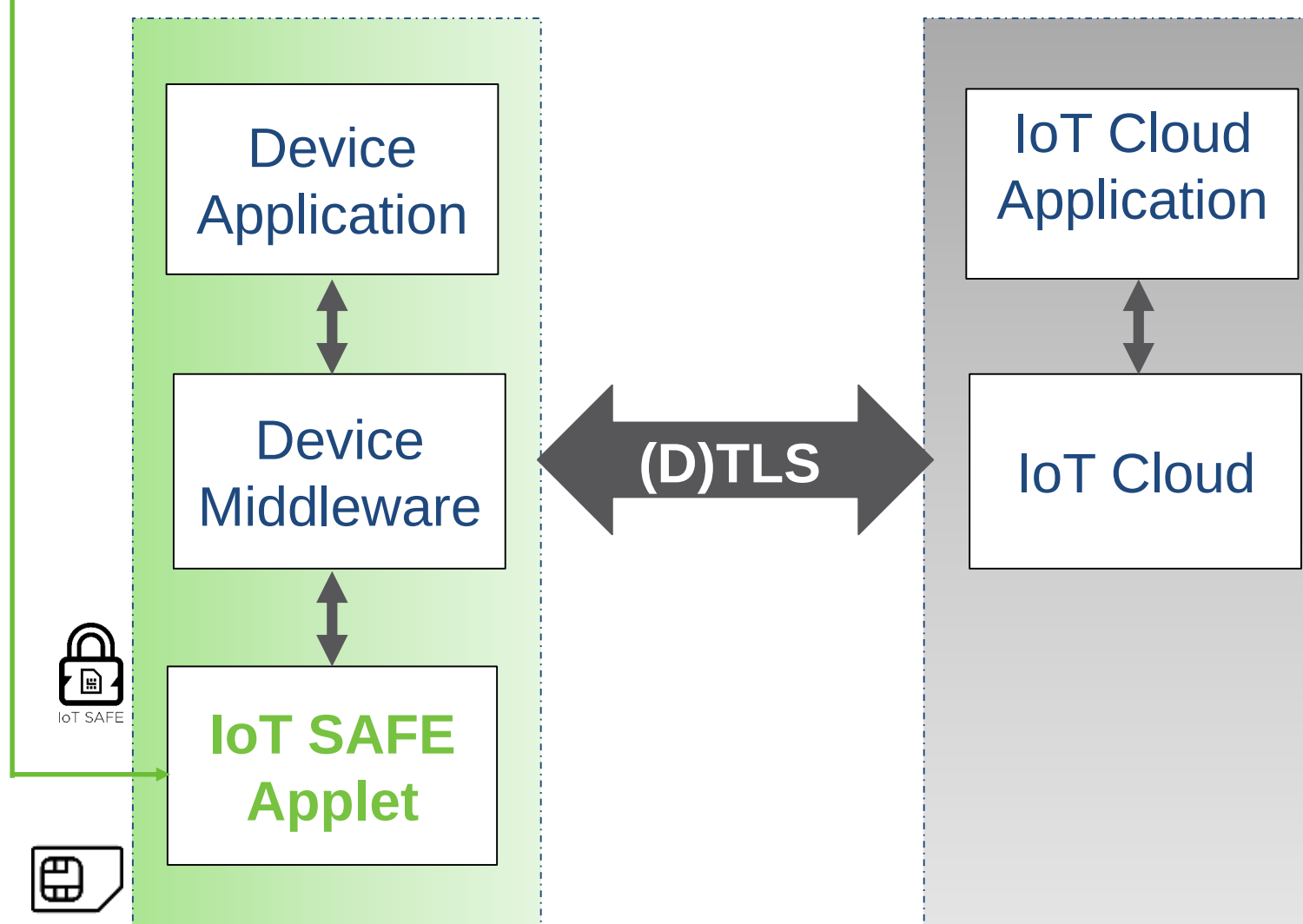
First focus: cellular connectivity



How do we achieve this?

(e)SIM as a crypto box

- Present in every single cellular device
- Fully standardised
- Tamper resistant
- Crypto features
- Form factor agnostic





IoT SAFE

Lets Talk the Same Language

What do we want?

Security: deliver a set of security services to enable specific use cases

Homogeneity: achieve a solution which can be implemented ubiquitously across all device hardware from all different vendors

Scalability: have all players talking the same language to remove device fragmentation barrier

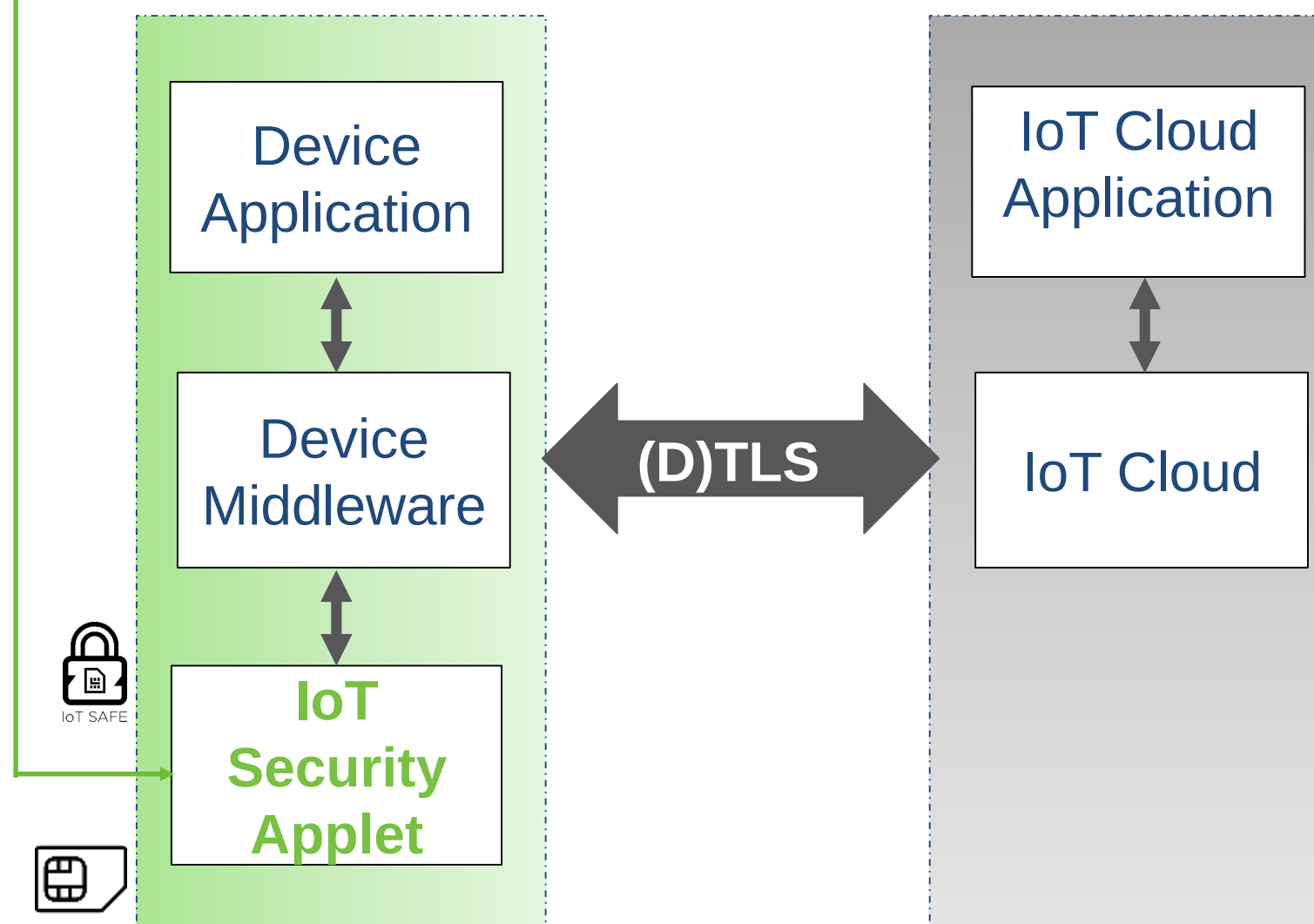
First focus: address device fragmentation



How do we achieve this?

(e)SIM as a crypto box

- Execution of specified set of security services
- Specified device to applet interface
- <https://www.gsma.com/iot/wp-content/uploads/2019/12/IoT.05-v1-IoT-Security-Applet-Interface-Description.pdf>





IoT SAFE

It Must be SIMple

What do we want?

Security: deliver a set of security services to enable specific use cases

Homogeneity: achieve a solution which can be implemented ubiquitously across all device hardware from all different vendors

Scalability: have all players talking the same language to remove device fragmentation barrier

Life cycle management:

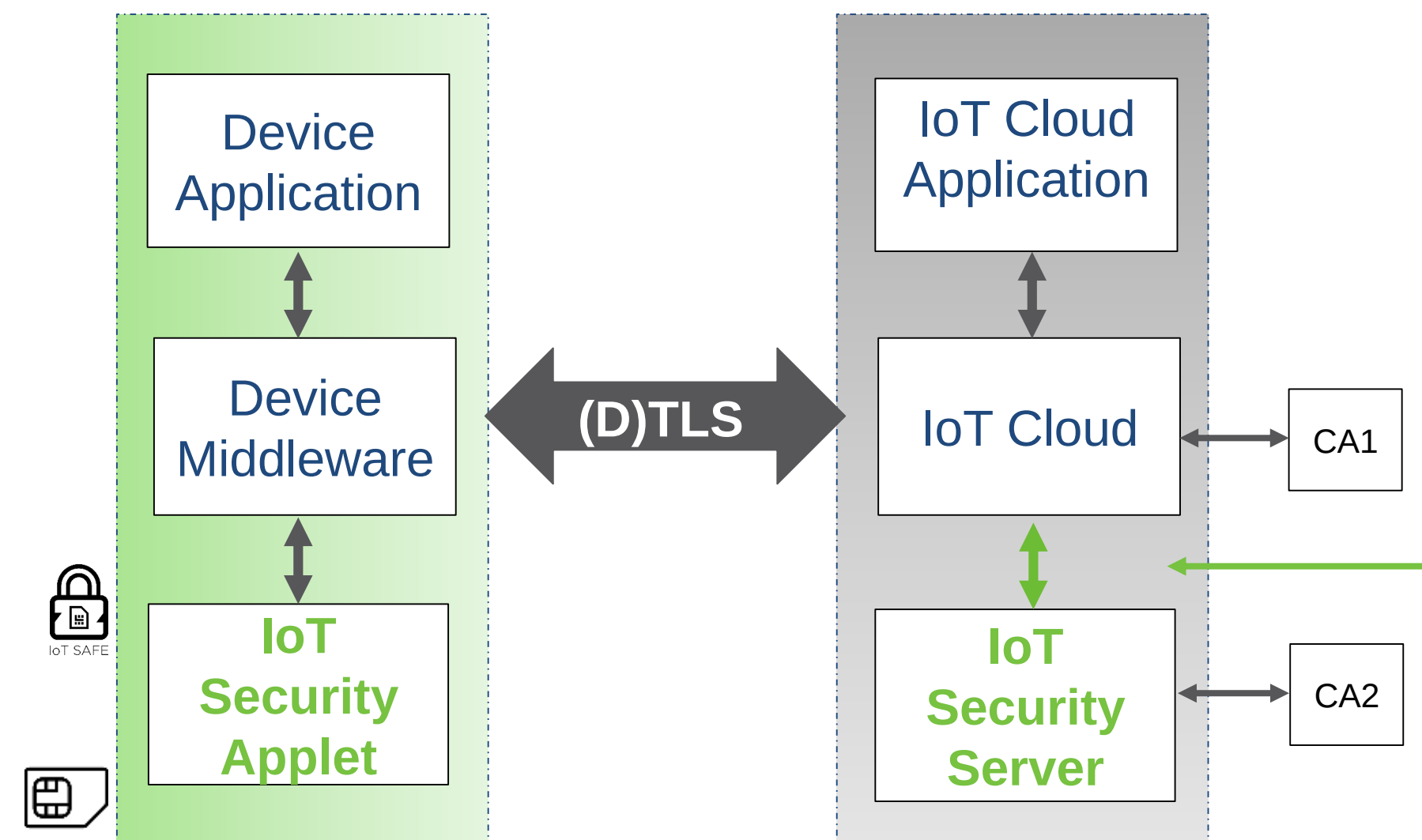
- Zero touch provisioning
- Ensure it is possible to create new/additional identities and renew, revoke them



How do we achieve this?

IoT Security Server

- Applet and Cloud automatic provisioning at switch on
- Lifecycle management (create, add, renew, revoke)
- Cloud agnostic
- Pre-defined and specified API
- Comply with different CA requirements





IoT SAFE

Adapted to Specific Constraints

What do we want?

Security: deliver a set of security services to enable specific use cases

Homogeneity: achieve a solution which can be implemented ubiquitously across all device hardware from all different vendors

Scalability: have all players talking the same language to remove device fragmentation barrier

Life cycle management:

- Zero touch provisioning
- Ensure it is possible to create new/additional identities and renew, revoke them

Cost effectiveness: serve high/mid range IoT devices but also constrained devices

How do we achieve this?

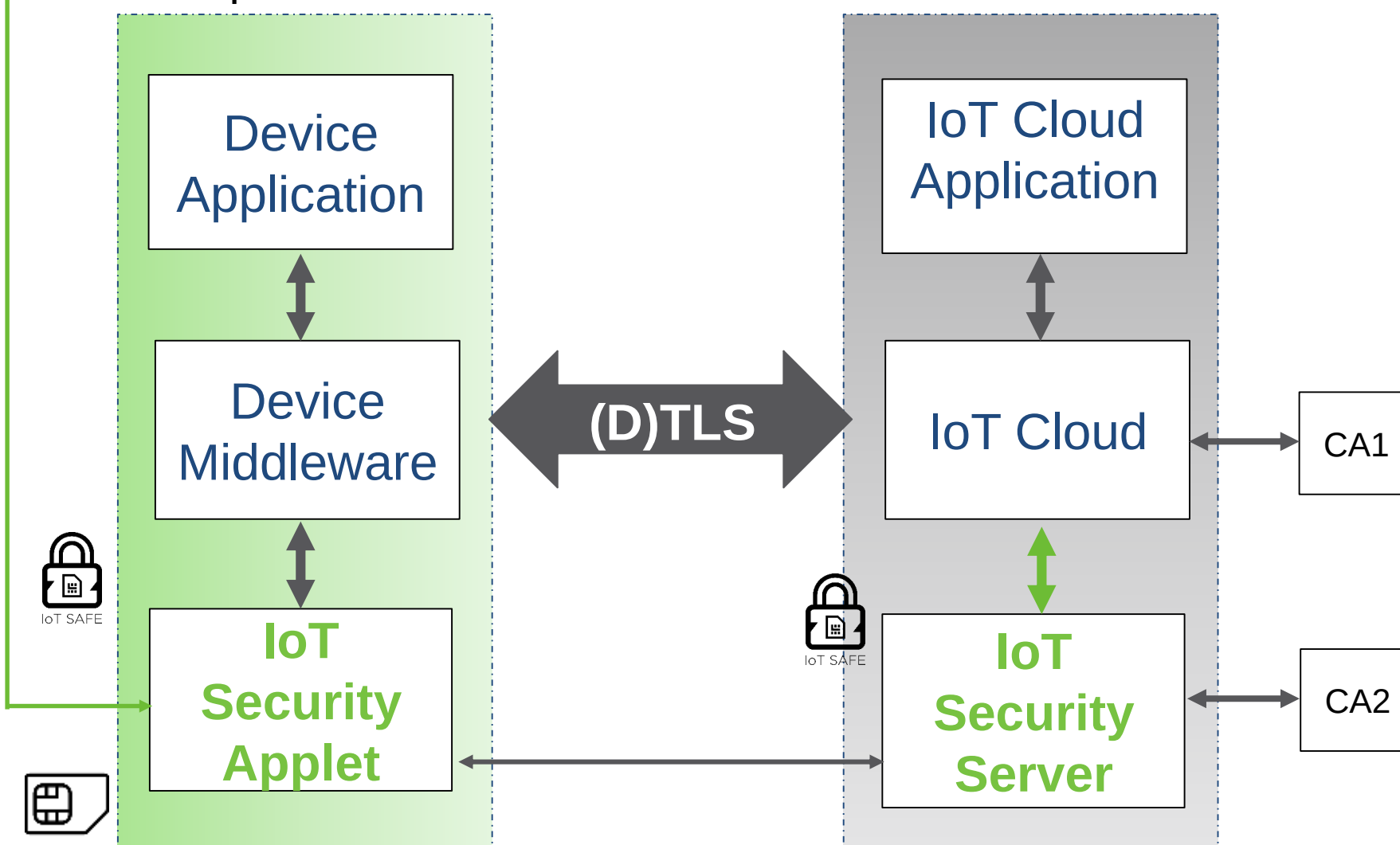
(e)SIM as a crypto box

Applet #1

- PKI
- ECC mandatory
- RSA optional
- PSK optional

Applet #2

- PSK only





IoT SAFE

Thank you and be SAFE



<https://www.trustedconnectivityalliance.org>



@TCAlliance_



<https://uk.linkedin.com/company/TrustedConnectivityAlliance>