Facing the Challenges of M2M Security and Privacy

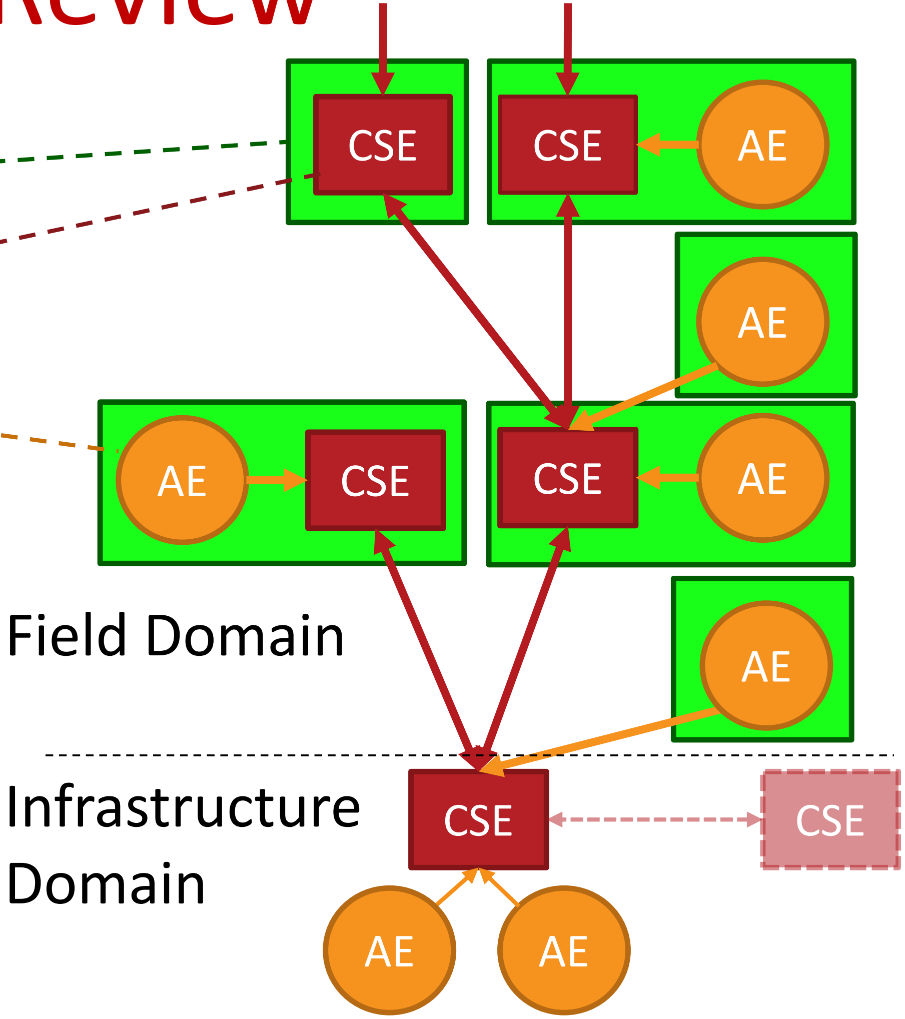
Phil Hawkes
Principal Engineer at Qualcomm Inc.
phawkes@qti.qualcomm.com
oneM2M www.oneM2M.org

Overview

- oneM2M Architecture: a quick review
- Challenges
  1. Large variety of scenarios
  2. Any device in any deployment
  3. A device cannot make autonomous “judgment calls” on privacy
- Solutions
  A. Secure communication
  B. Remote provisioning
  C. Access control policies
- Future Challenges

oneM2M Architecture: A Quick Review

- Entities
  - Nodes (=Devices)
  - Common Service Entity (CSE)
  - Application Entity (AE)
- Interactions:
  - Mca: AE-to-CSE
  - Mcc, Mcc’: CSE-to-CSE
  - RESTful
- For more info see webinar Taking a look inside oneM2M



Challenges

1. Large variety of scenarios
2. Any device in any deployment
3. A device cannot make autonomous "judgment calls" on privacy

Challenges

1. Large variety of deployments
   - "Assets" that need protecting can be unique to a deployment
     - Content confidentiality, content integrity, anonymity, traffic efficiency
   - Environment can be unique to a deployment
     - Does wired or wireless transport layer provide adequate security?
     - Tamper-resistance considerations
   - *(Continued on next slide)*
2. Any device in any deployment
3. A device cannot make autonomous "judgment calls" on privacy

Challenges

1. Large variety of deployments (continued)
   - Variety of authentication scenarios
     - Pre-shared Key provisioned to both by end-points
     - PKI/Certificates (asymmetric cryptography)
     - Centralized authentication
2. Any device in any deployment
3. A device cannot make autonomous "judgment calls" on privacy

Challenges

1. Large variety of deployment scenarios
2. Any device in any deployment
   - Interoperability: agree on minimal set of cipher suites
   - Credential management
     a. Provisioning at manufacture
     b. Human-assisted provisioning during deployment
        - e.g. manual entry, via USB
     c. Remote provisioning of fielded devices
     d. Derivation from pre-existing credentials (e.g. transport network)

     Note: a, b are enabled but not specified by oneM2M
3. A device cannot make autonomous "judgment calls" on privacy

Challenges

1. Large variety of scenarios
2. Any device in any deployment
3. A device cannot make autonomous “judgment calls” on privacy
   – M2M/IoT may expose information about our lives without our awareness
   – Privacy = who can access information about me
   – CSE needs to determine: “Should I allow access?”
   – Can’t ask human to make case-by-case judgment call
   – **CSE needs clear rules**

Challenges & Solutions

1. Large variety of scenarios
2. Any device in any deployment
3. A device cannot make “judgment calls” on privacy

A. Secure communication

various authentication options

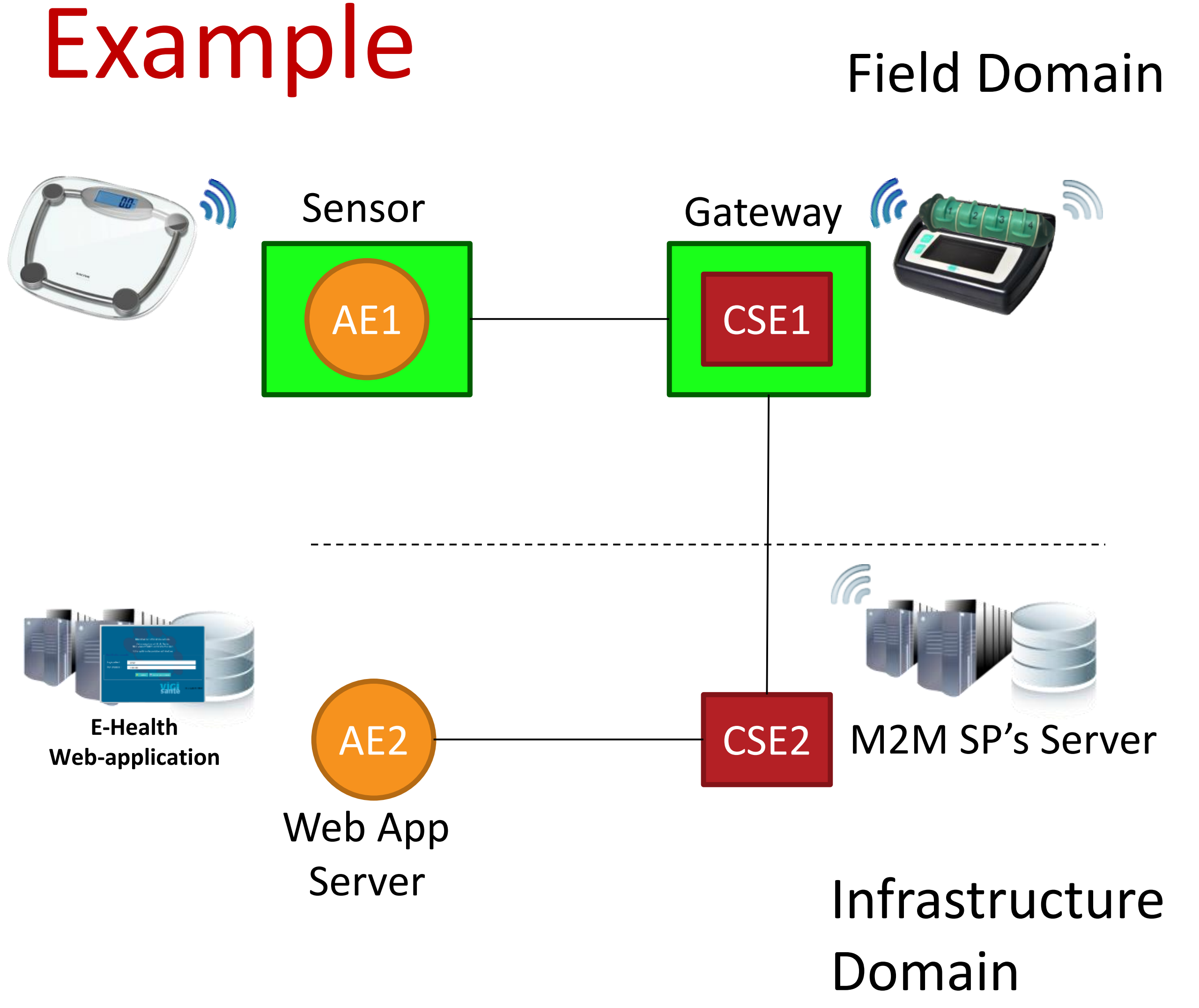
B. Remote provisioning

various authentication options

C. Access Control Policies

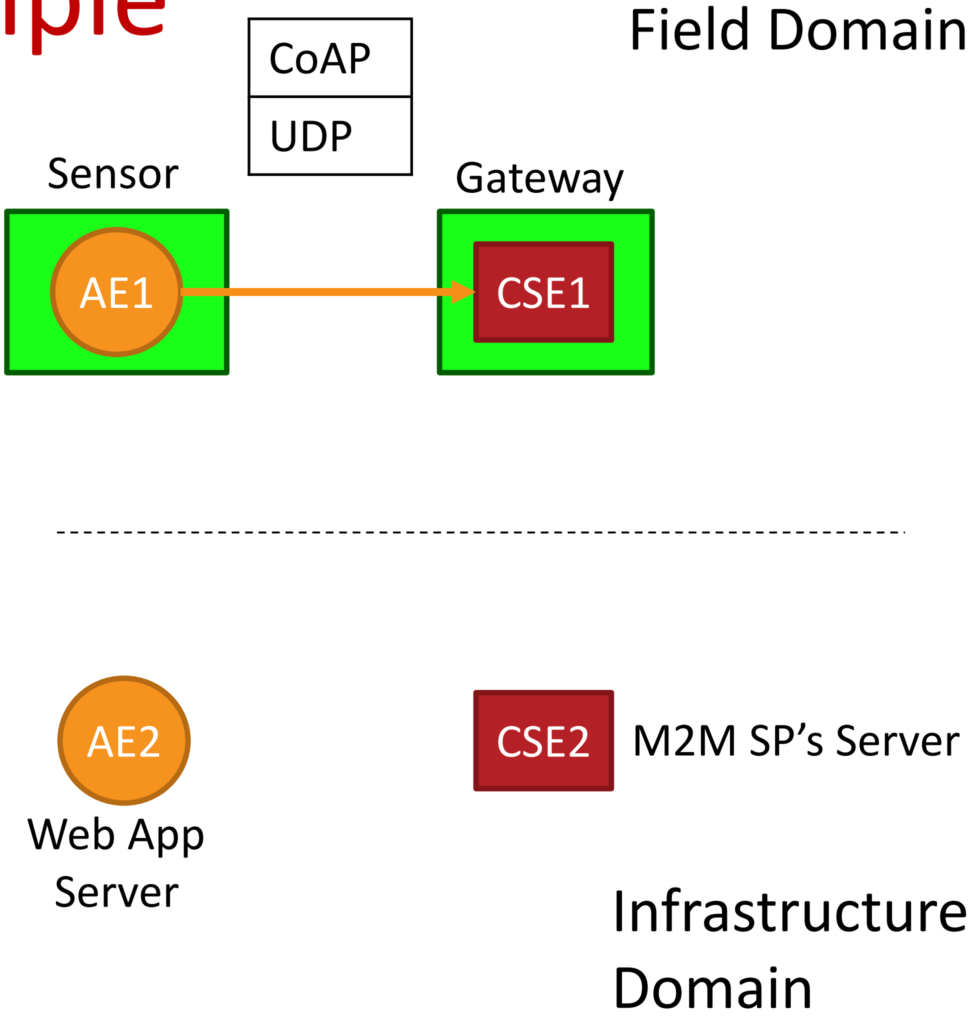
expresses wide variety of rules

Secure Communication: Example



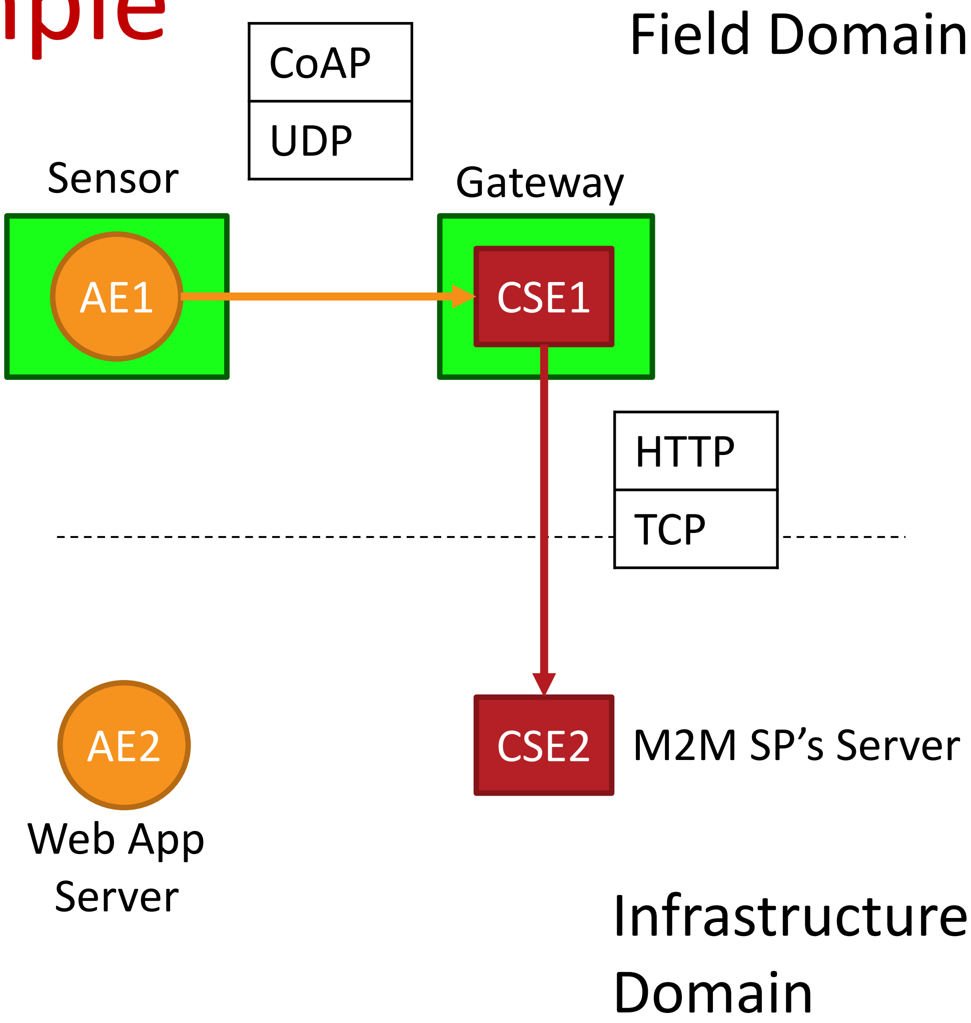
Secure Communication: Example

1. AE1 passes sensor reading to CSE1



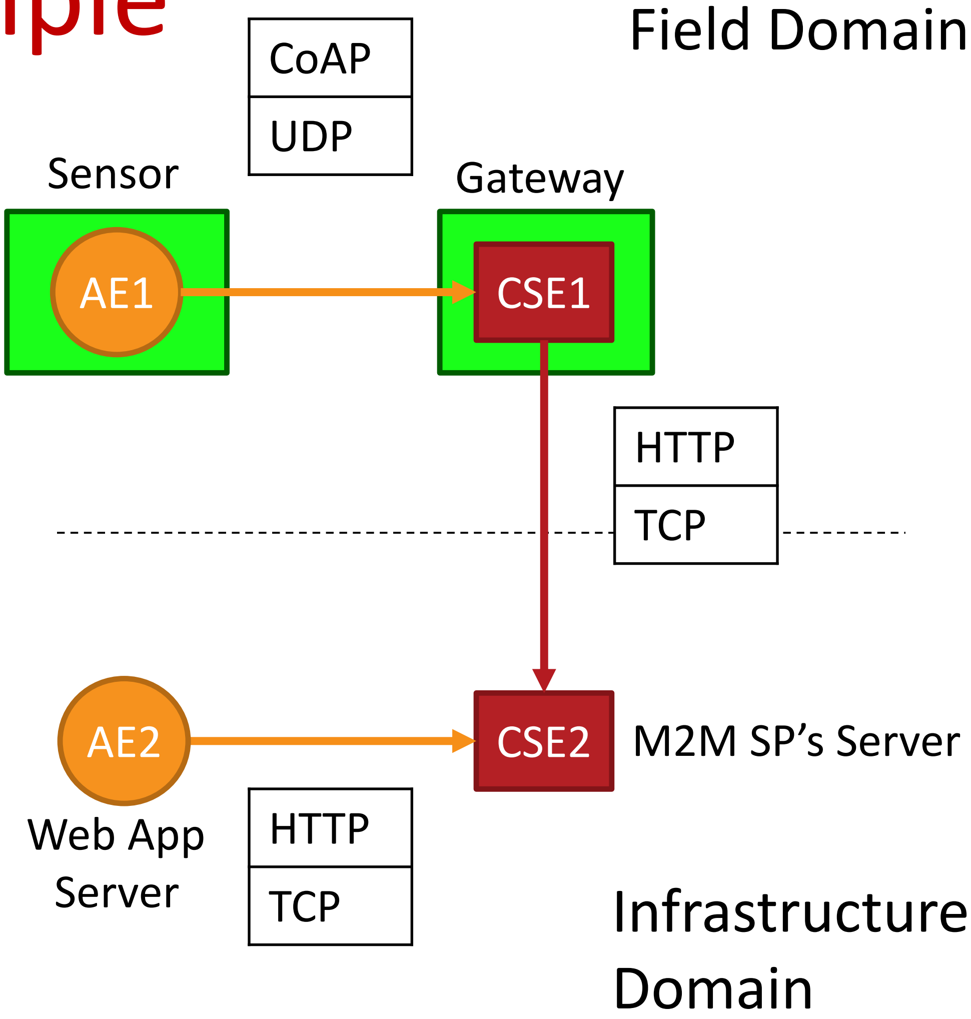
Secure Communication: Example

1. AE1 passes sensor reading to CSE1
2. CSE1 forwards sensor reading to CSE2



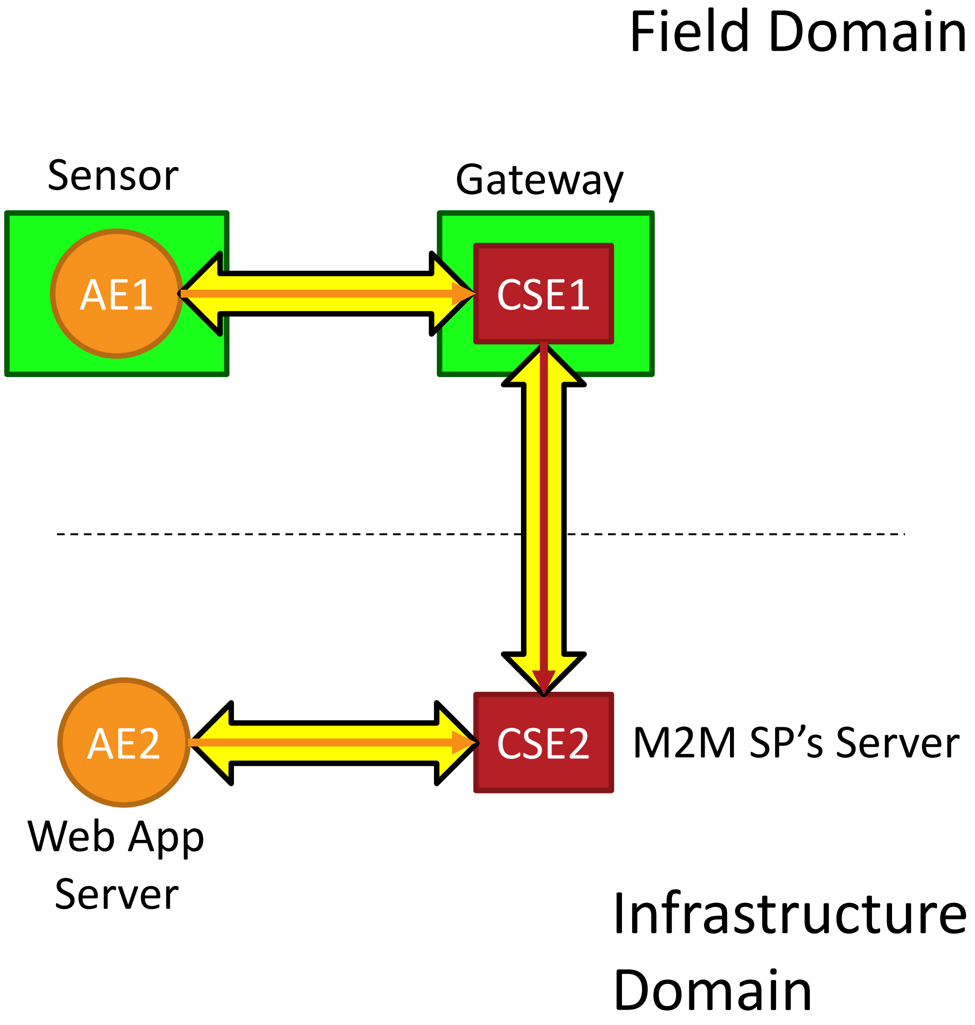
Secure Communication: Example

1. AE1 passes sensor reading to CSE1
2. CSE1 forwards sensor reading to CSE2
3. AE2 retrieves sensor reading from CSE2



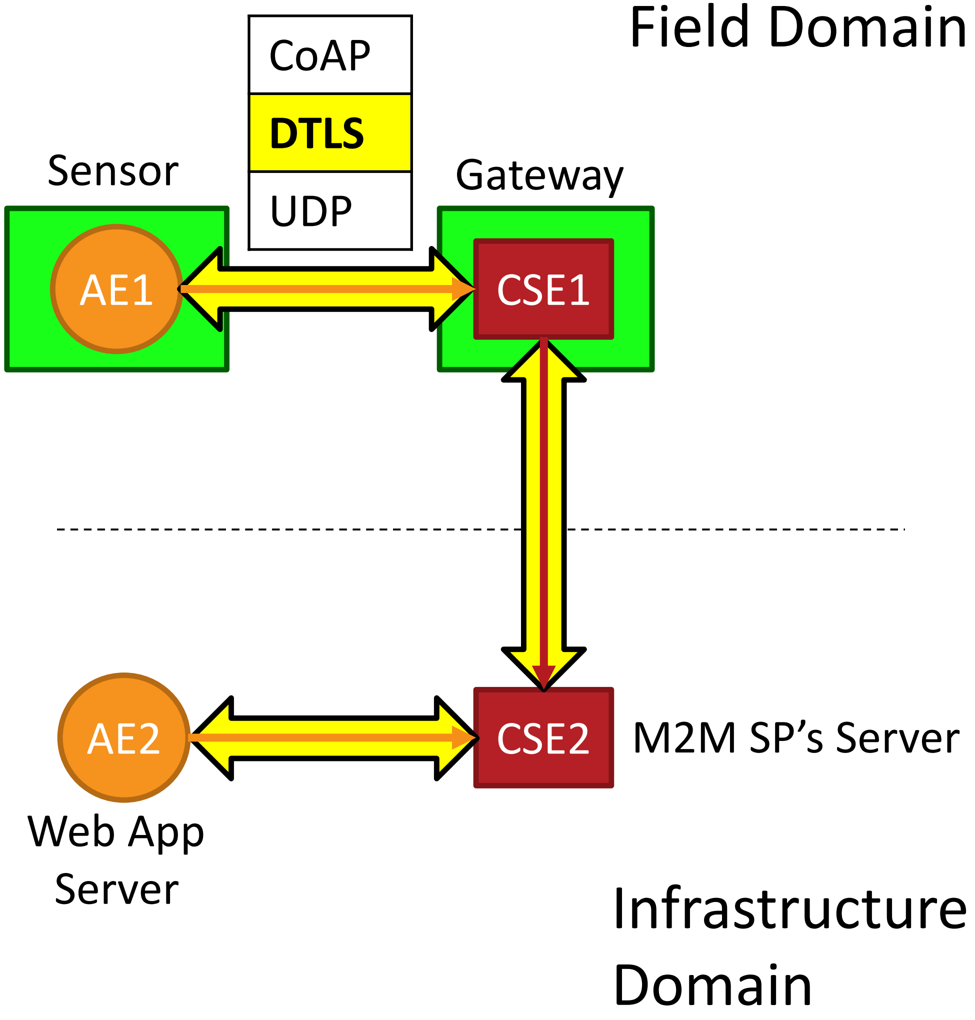
Secure Communication

- Hop-by-Hop
  - Transited CSEs see clear text
  - Trusted to behave



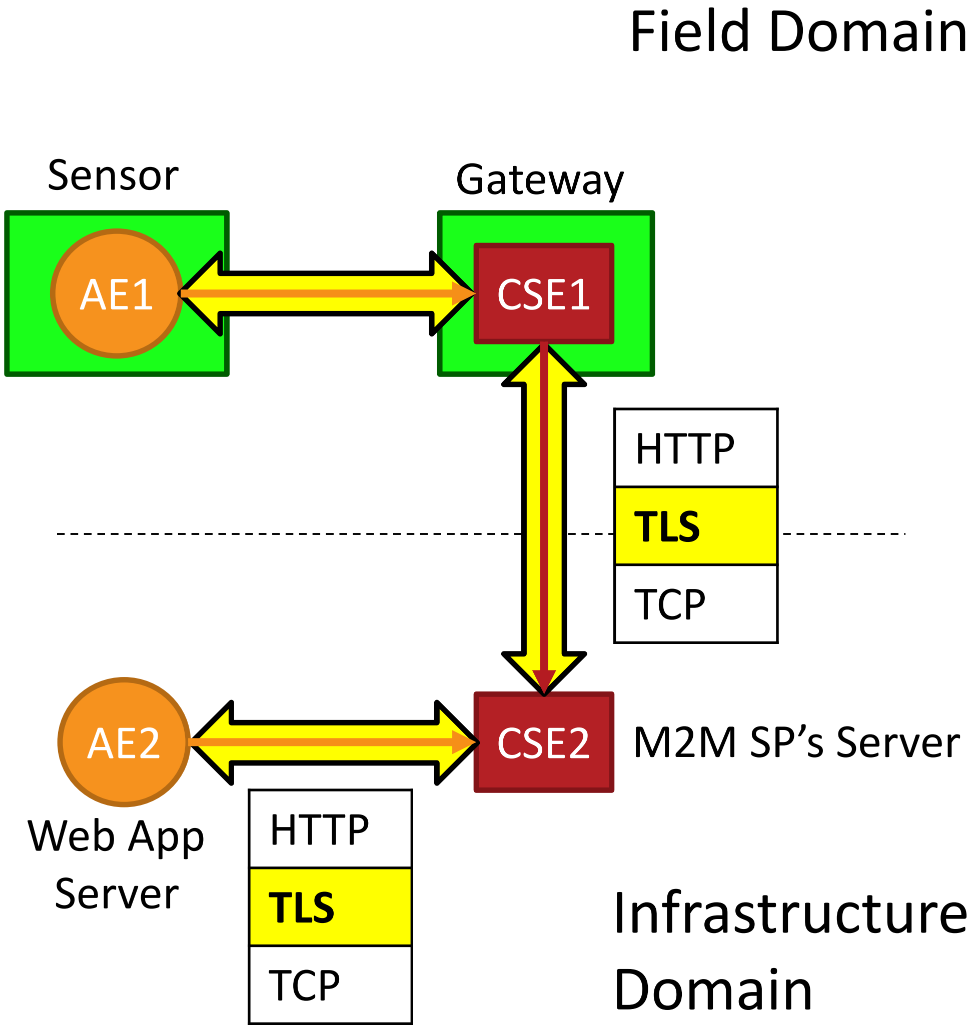
Secure Communication

- Hop-by-Hop
- TLS/DTLS v1.2
  - DTLS if UDP transport



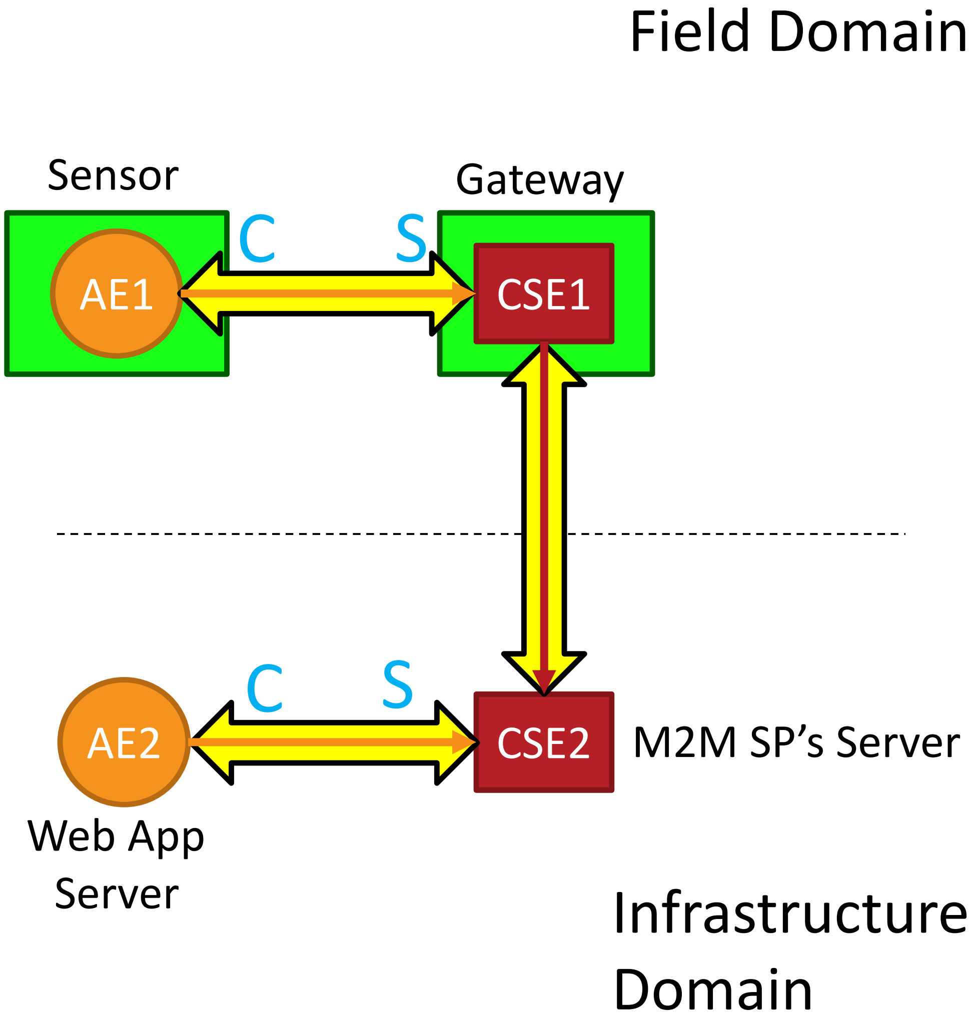
Secure Communication

- Hop-by-Hop
- TLS/DTLS v1.2
  - DTLS if UDP transport
  - TLS if TCP transport
  - *Sometimes write (D)TLS or just TLS for both*



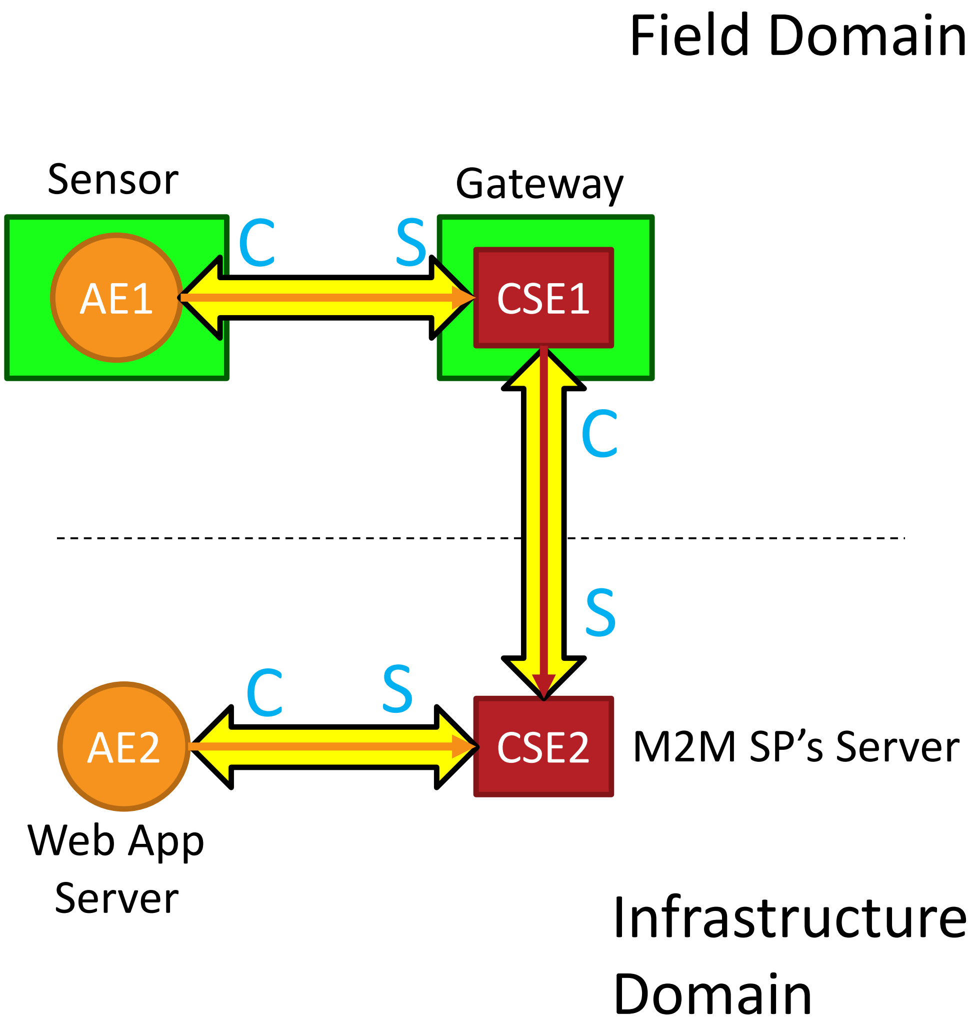
Secure Communication

- Hop-by-Hop
- TLS/DTLS v1.2
- AE-CSE
  - AE: TLS Client (C)
  - CSE: TLS Server (S)



Secure Communication

- Hop-by-Hop
- TLS/DTLS v1.2
- AE-CSE
  - AE: TLS Client (C)
  - CSE: TLS Server (S)
- CSE-CSE
  - CSE1: TLS Client (C)
  - CSE2: TLS Server (S)



Authentication Options

- Pre-Shared Key (PSK)
  - TLS Client & Server provisioned with a shared key#
- Certificate
  - TLS Client & Server both have certificates
- M2M Authentication Function (MAF)
  - MAF operated by 3rd Party or M2M Service Provider
  - TLS Client and MAF provisioned with a shared key#
  - MAF assists authentication of TLS Client & Server

#This shared key can be remotely provisioned

Certificates

- Somewhat aligned with CoAP Security RFC7252
- X.509/PKIX (RFC 5280)
- RawPublicKey Certificates
  - Contains only X.509 SubjectPublicKeyInfo element
  - Suits less complex deployments & debugging
- Certificates chaining to a trust anchor. E.g.
  - Device Certificate (e.g. manufacturer issued)
  - M2M SP issued certificate identifying CSE or AE

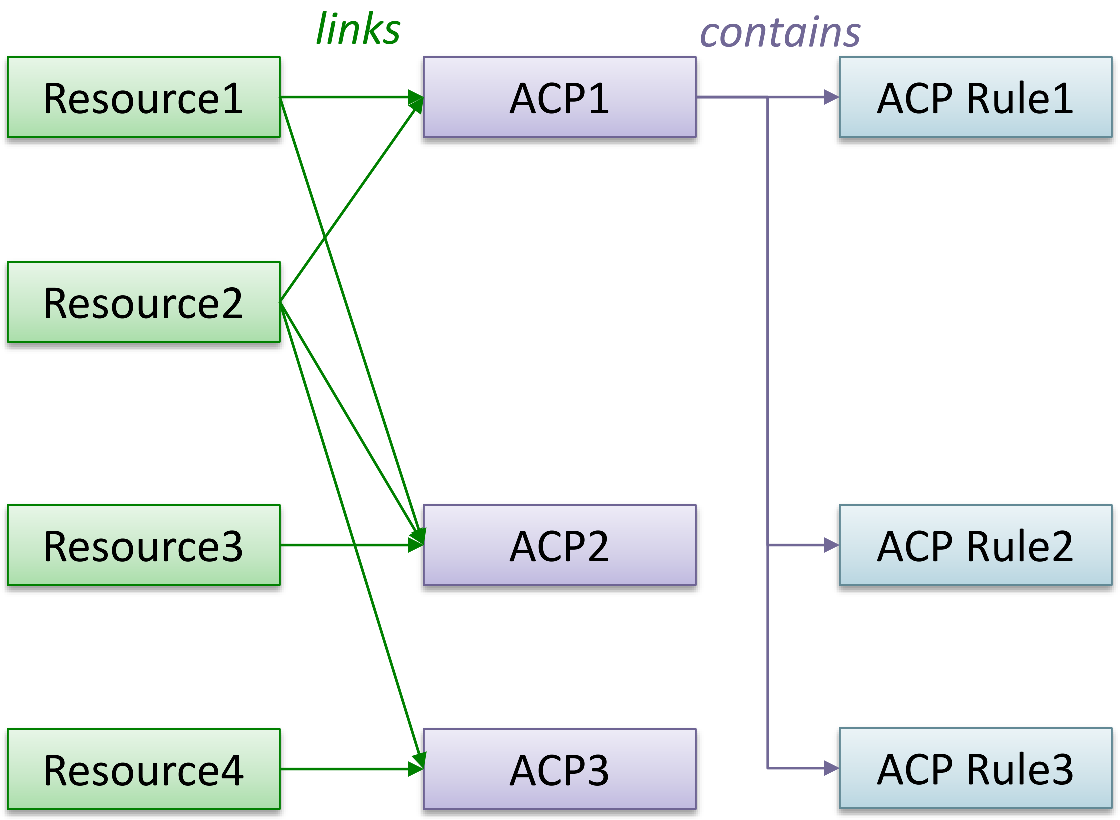
Remote Provisioning

- Process provisioning a shared key to two entities
- M2M Enrolment Function (MEF)
  - Assists remote provisioning
  - Operated by 3rd Party or M2M Service Provider
- Mechanisms for establishing shared key
  - *TLS Client & MEF perform (D)TLS, export shared key*
    - PSK
    - Certificates
  - Derived from Network Access credentials
    - Network Access Provider assists in mutual authentication
    - Generic Bootstrapping Architecture (GBA) 3GPP TS 33.220

Access Control Requirements

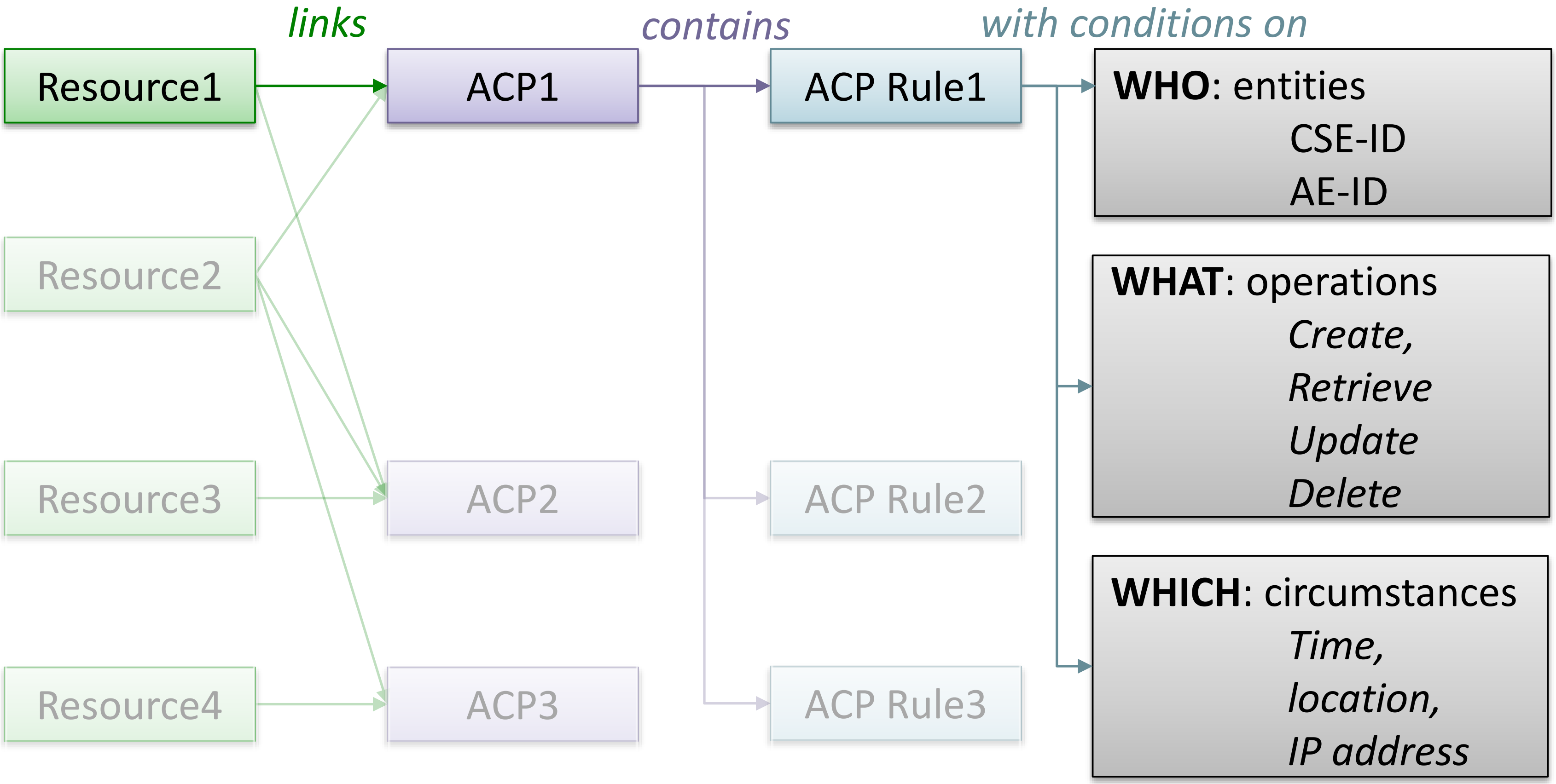
- oneM2M uses a RESTful architecture
  - – API: request to perform an operation on a resource
  - – Operations: Create, Retrieve, Update, Delete
  - – Webinar Taking a look inside oneM2M has more info
- CSEs can’t make resource access judgement calls
- CSE need clear rules dictating, for each resource
  - – **WHO** (which CSEs and AEs) are authorized to access,
  - – **WHAT** operations (see above), and under…
  - – **WHICH** circumstances (e.g. time, location of entity)

Access Control Policies (ACP) Resources



Resource access is authorized upon satisfying at least one ACP rule in one of the linked ACPs

Access Control Policies (ACP) Resources



ACP rule is satisfied if WHO and WHAT and WHICH are satisfied by requesting entity, requested operation and circumstances

oneM2M Security Documents

- TR-0008 “Analysis of Security Solutions for the oneM2M System”

  http://onem2m.org/images/files/deliverables/oneM2M_TR-0008-Security-V1_0_0.doc

- TS-0003 “Security Solutions”

  http://onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf

- Latest versions available from

  ftp://ftp.onem2m.org/Work%20Programme/WI0007/

Limitations of initial release

- A “minimum deployable solution” addressing short term needs
- Focus: Vertically deployed industrial applications
  - Centralized client-server architectures
  - Most devices have limited number of static connections
  - Deployments are managed by skilled workforce
  - Nodes are trusted to behave
- Our solutions meet these needs while having a place in future M2M/IoT (consumer) scenarios

Future Challenges

- Decentralization
  - Increasingly complex interactions
    - Sharing Information between deployments
    - Complex authentication and authorization scenarios
    - Confidentiality & integrity concerns
  - Unskilled Consumers managing their “Things”
- Technological Challenges:
  - End-to-End (multi-hop) message security
  - Many connections per device
  - Authentication & Authorization mechanisms

Conclusion:

Challenges & Solutions

1. Large variety of scenarios	A. Secure communication various authentication options
2. Any device in any deployment	B. Remote provisioning various authentication options
3. A device cannot make “judgment calls” on privacy	C. Access Control Policies expresses wide variety of rules

Join us for the next webinar

“On Management, Abstraction & Semantics”

by Dr. Yongjing Zhang

Standard Research Project Lead
at Huawei Technologies Co., Ltd

27 November 2014 at 0700 UTC

http://www.onem2m.org/btchannel.cfm

Check out the recorded webinars

“How standardization enables the next internet evolution”

by Marc Jadoul

Strategic Marketing Director, Alcatel-Lucent

“Taking a look inside”

by Nicolas Damour

Senior Manager for Business and Innovation Development, Sierra Wireless

http://www.onem2m.org/btchannel.cfm

Join us at the oneM2M showcase event

- OneM2M project partners, rationale and goals
- OneM2M Service Layer Specification release
- Showcase demos that demonstrate oneM2M “live"

9 December 2014, Sophia-Antipolis, France

(free of charge, but online registration is required)

http://www.onem2m.org/Showcase

Followed by the ETSI M2M workshop

Q & A

Backup Slides

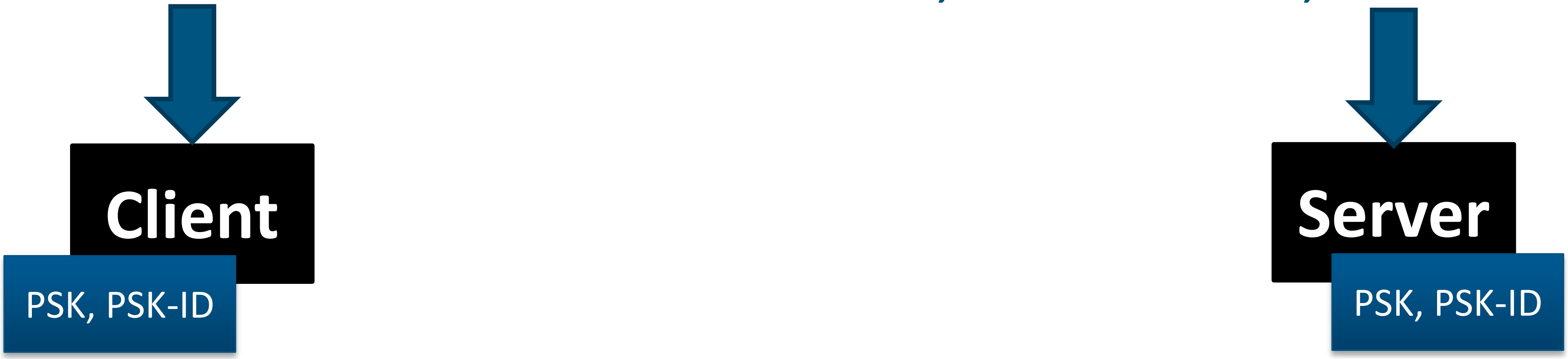
PSK-Based Authentication

Client

Server

PSK

1. Provision identical PSK, PSK-ID to A, B



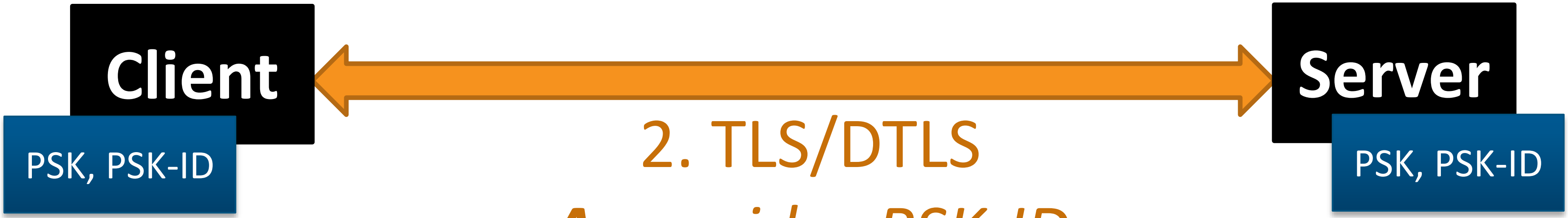
Client

PSK, PSK-ID

Server

PSK, PSK-ID

PSK

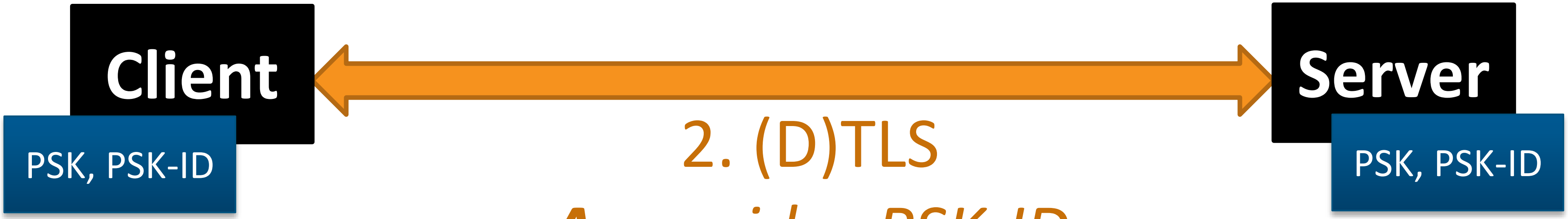


2. TLS/DTLS

***A** provides PSK-ID*

***B** identifies PSK from PSK-ID*

PSK



2. (D)TLS

***A** provides PSK-ID*

***B** identifies PSK from PSK-ID*

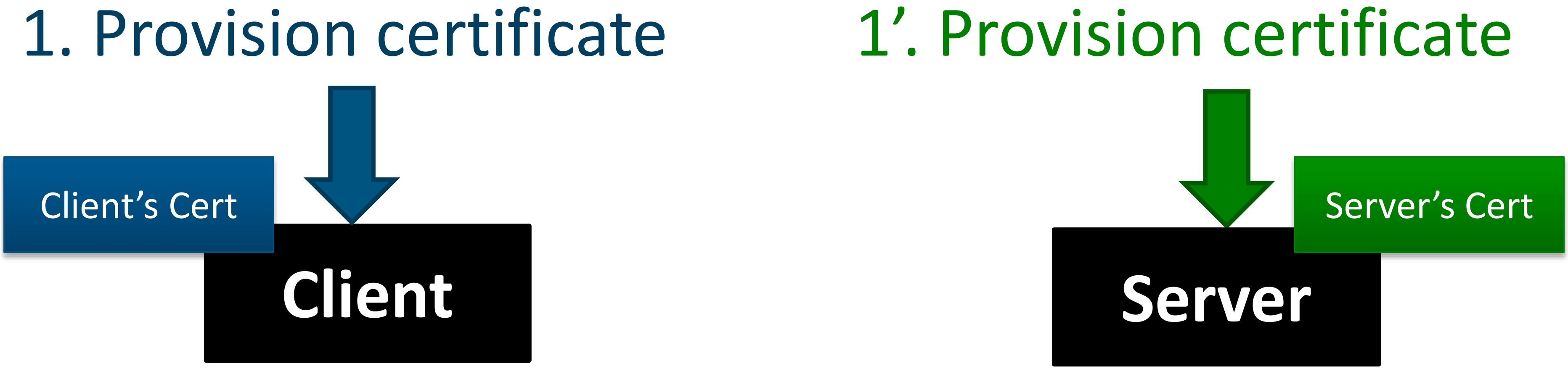
- **Advantages:**
  - Simple Concept
- **Challenges:**
  - May need multiple keys provisioned
  - Doesn’t scale well

PKI/Certificate-Based Authentication

Client

Server

PKI



1. Provision certificate

1’. Provision certificate

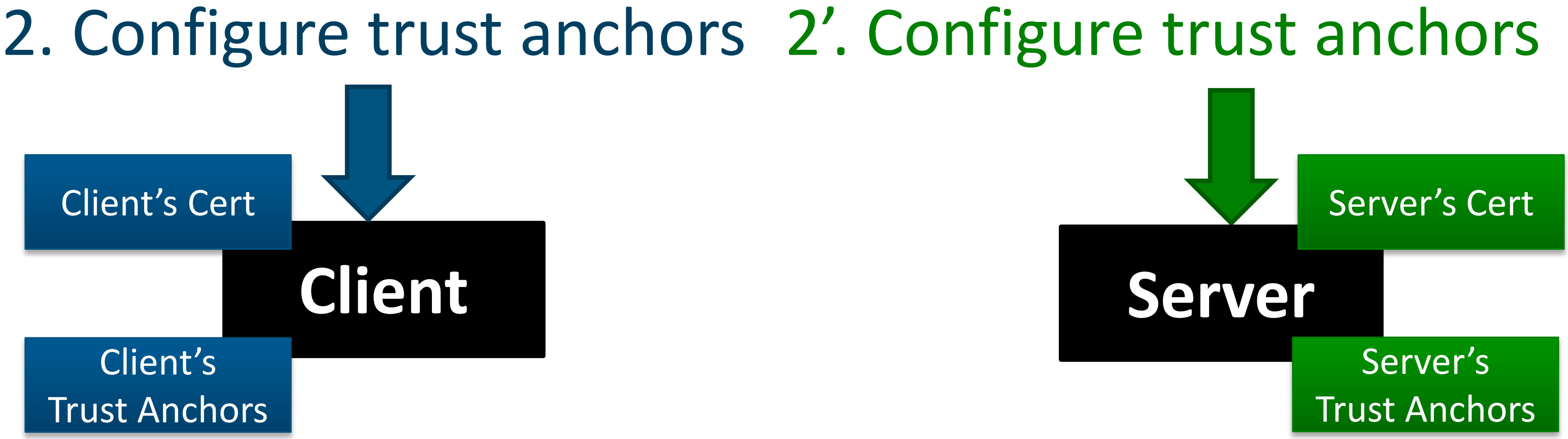
Client’s Cert

Client

Server

Server’s Cert

PKI



2. Configure trust anchors

2’. Configure trust anchors

Client’s Cert

Client

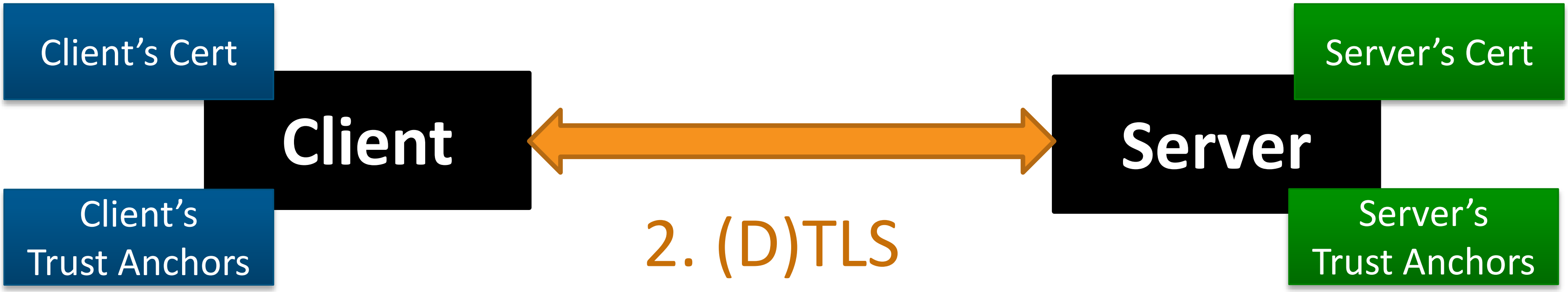
Client’s Trust Anchors

Server’s Cert

Server

Server’s Trust Anchors

PKI



Client's Cert

Client

Client's Trust Anchors

2. (D)TLS

Server's Cert

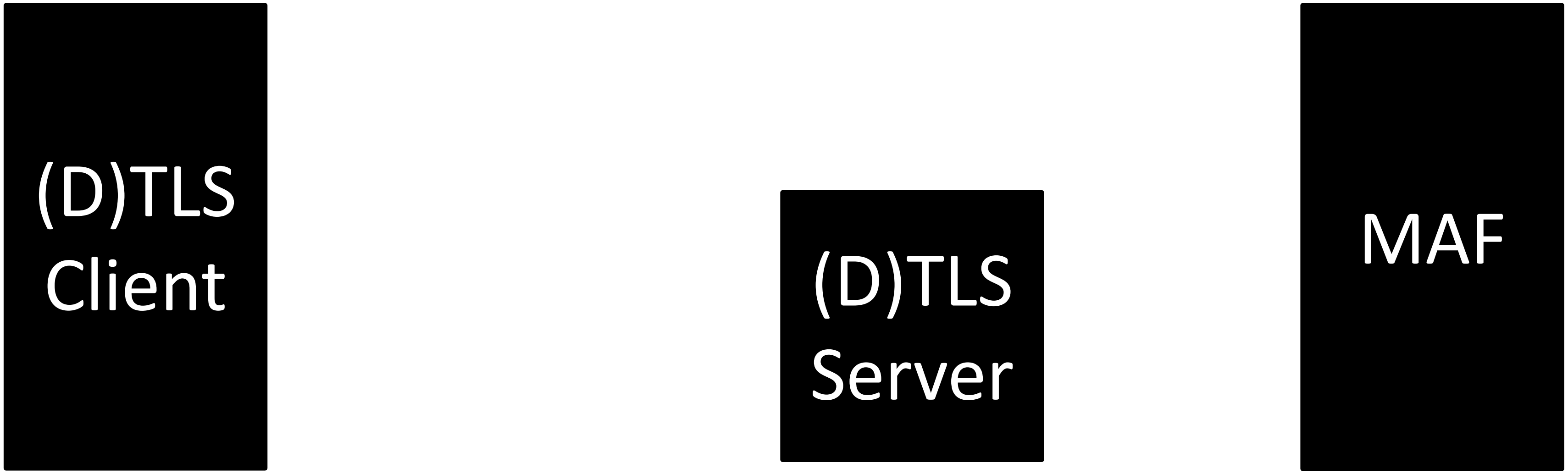
Server

Server's Trust Anchors

Validate **server's** cert against **client's** trust anchors

Validate **client** cert against **server's** trust anchors

MAF Assisted



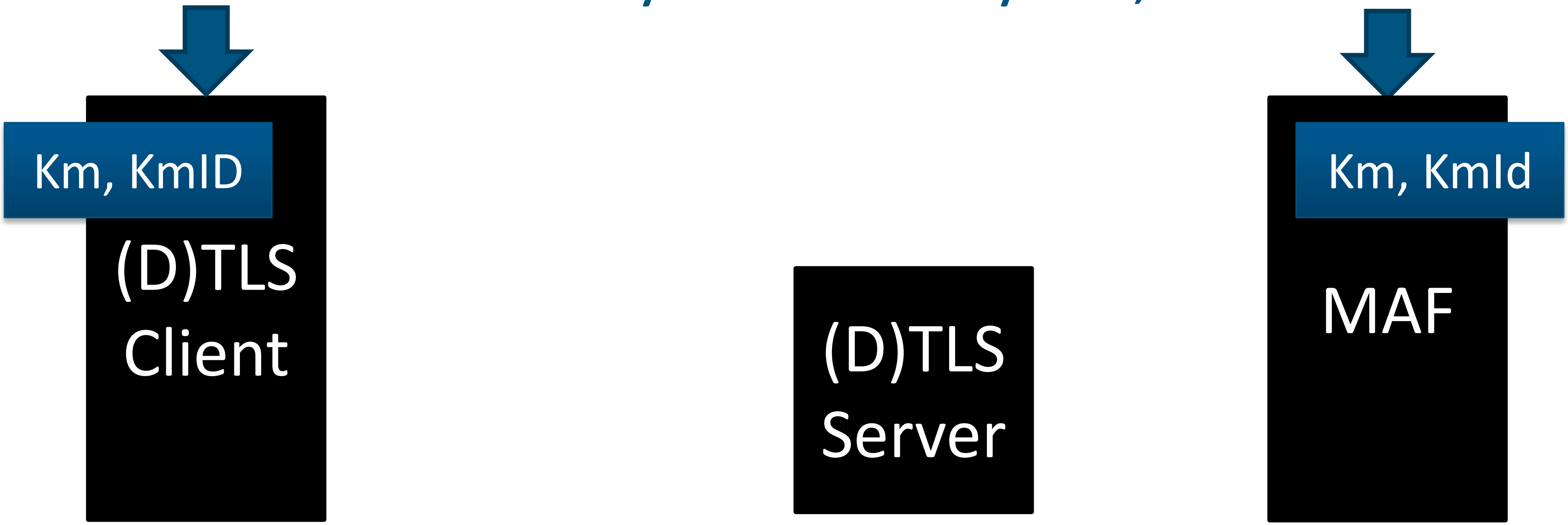
(D)TLS Client

(D)TLS Server

MAF

MAF Assisted

1. Provision symmetric key Km, KmId



Km, KmID

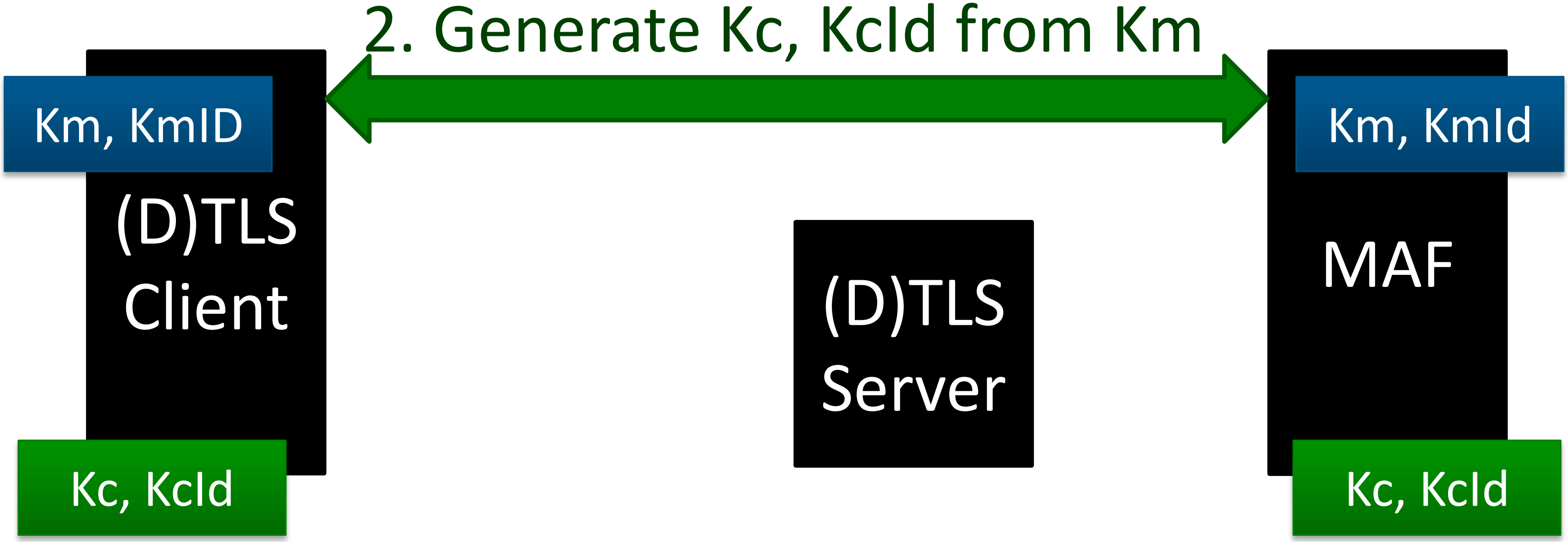
(D)TLS Client

(D)TLS Server

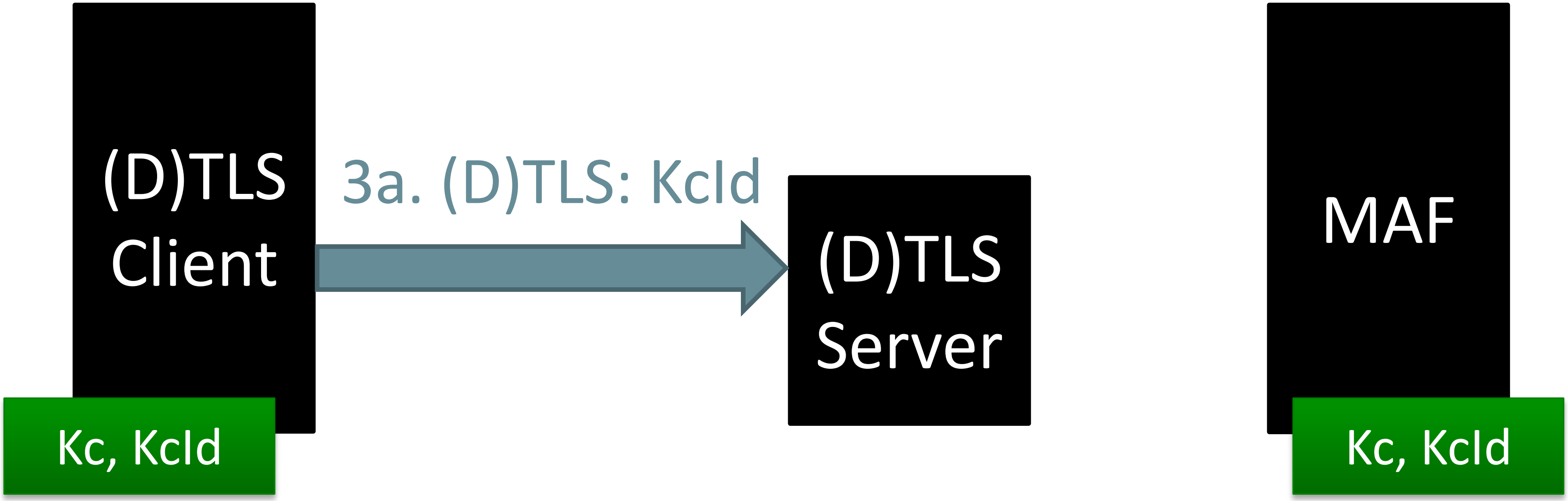
Km, KmId

MAF

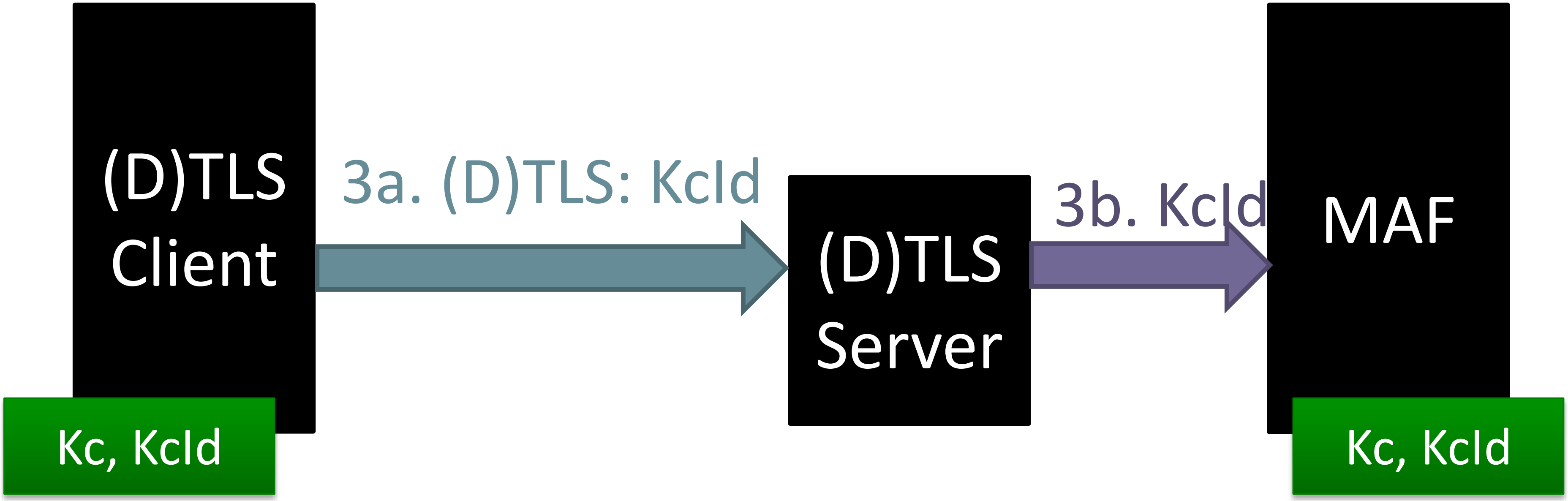
MAF Assisted



MAF Assisted



MAF Assisted



(D)TLS Client

Kc, KcId

3a. (D)TLS: KcId

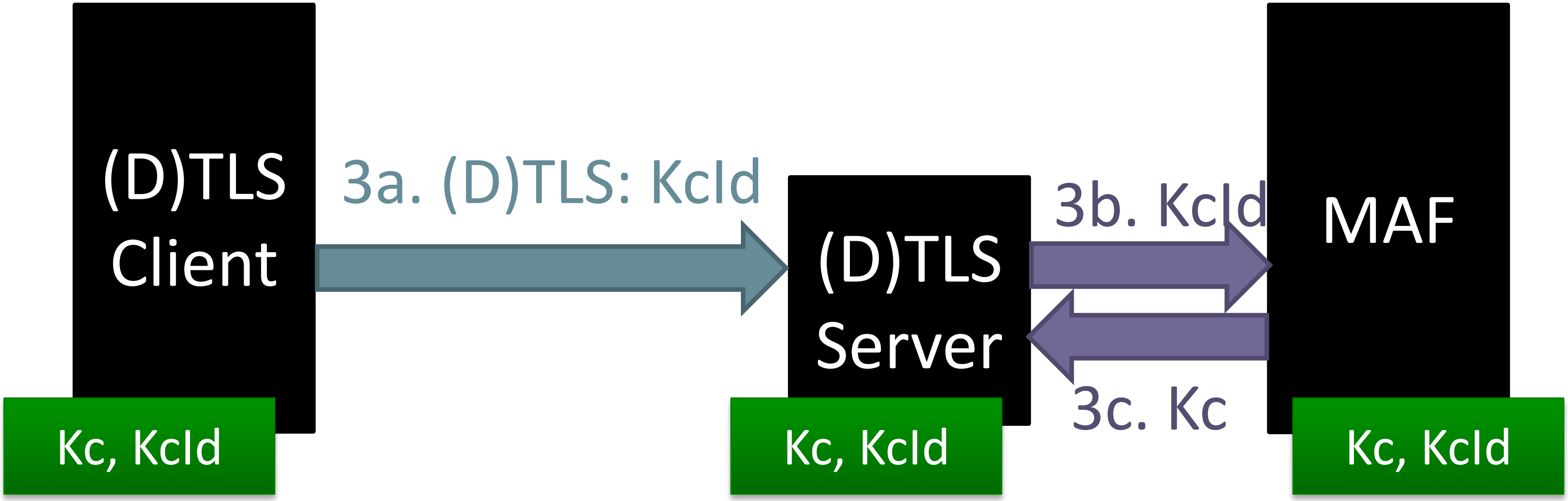
(D)TLS Server

3b. KcId

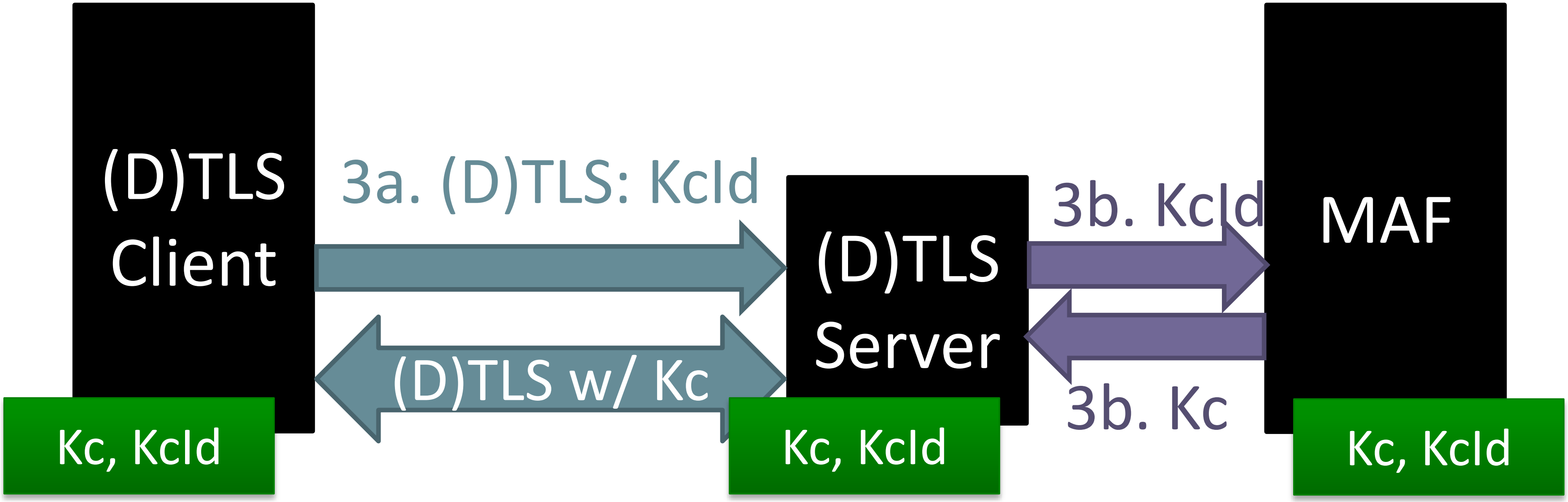
MAF

Kc, KcId

MAF Assisted



MAF Assisted



Remote Provisioning PArticipants

- Process provisions a shared key to two entities
- M2M Enrolment Function (MEF)
  - Assists remote provisioning
  - Operated by 3rd Party or M2M Service Provider
- Enrolee
  - Entity requesting to be provisioned
- Enrolment Target
  - Other entity that will ends up with the shared key

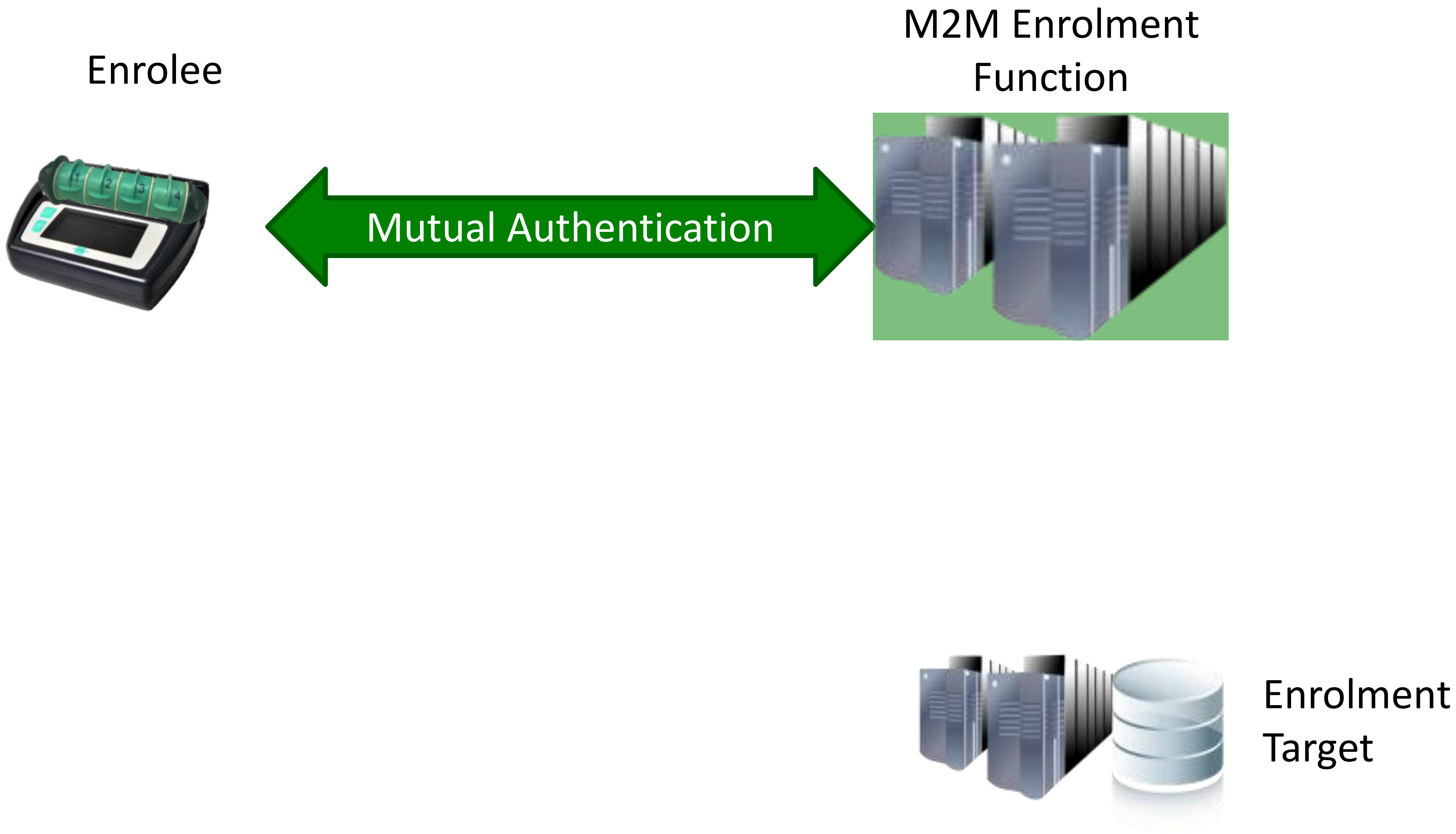
Remote Provisioning

Enrolee

M2M Enrolment Function

Enrolment Target

Remote Provisioning



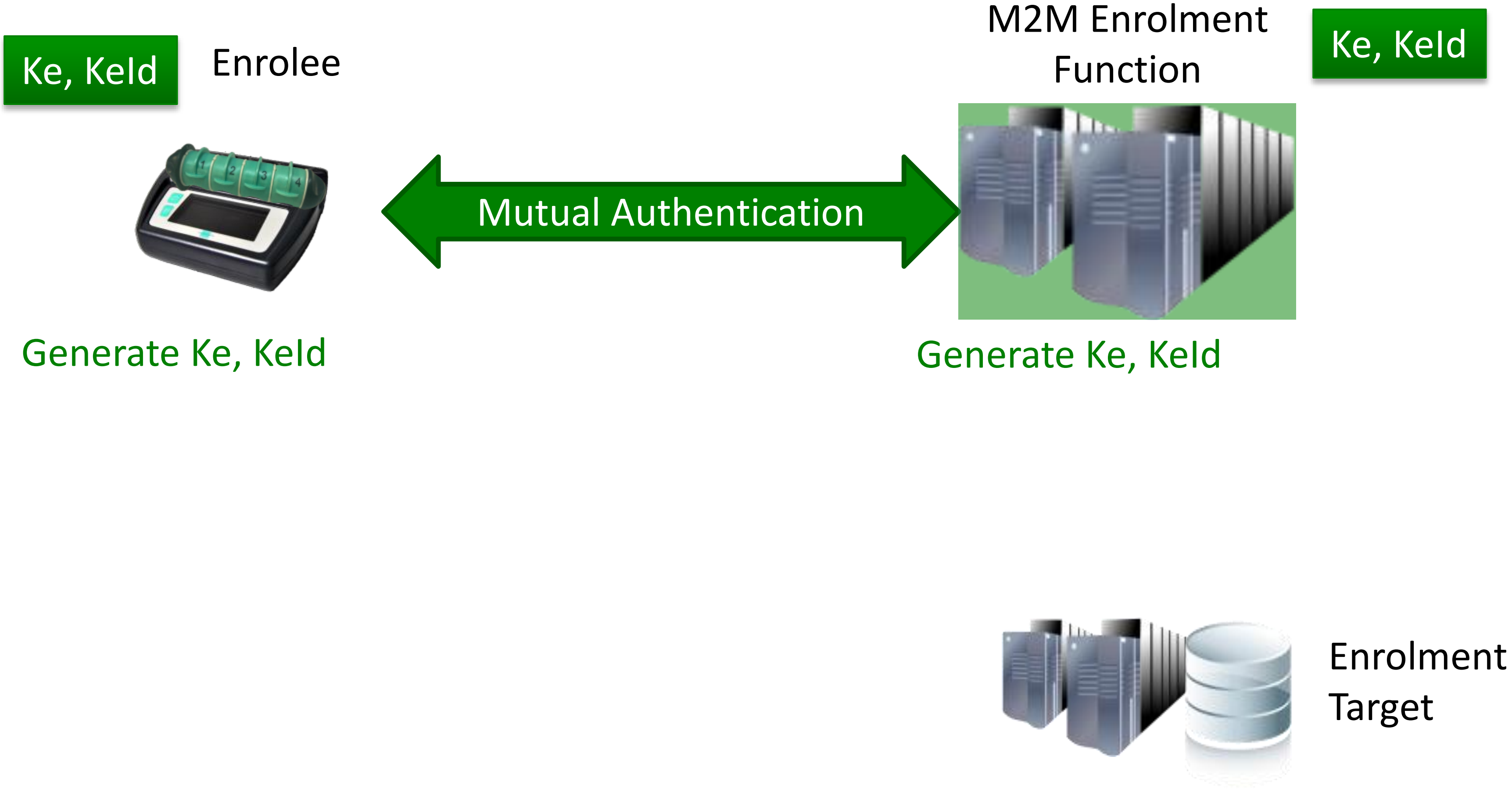
Enrolee

M2M Enrolment Function

Mutual Authentication

Enrolment Target

Remote Provisioning



Ke, KeId

Enrolee

M2M Enrolment Function

Ke, KeId

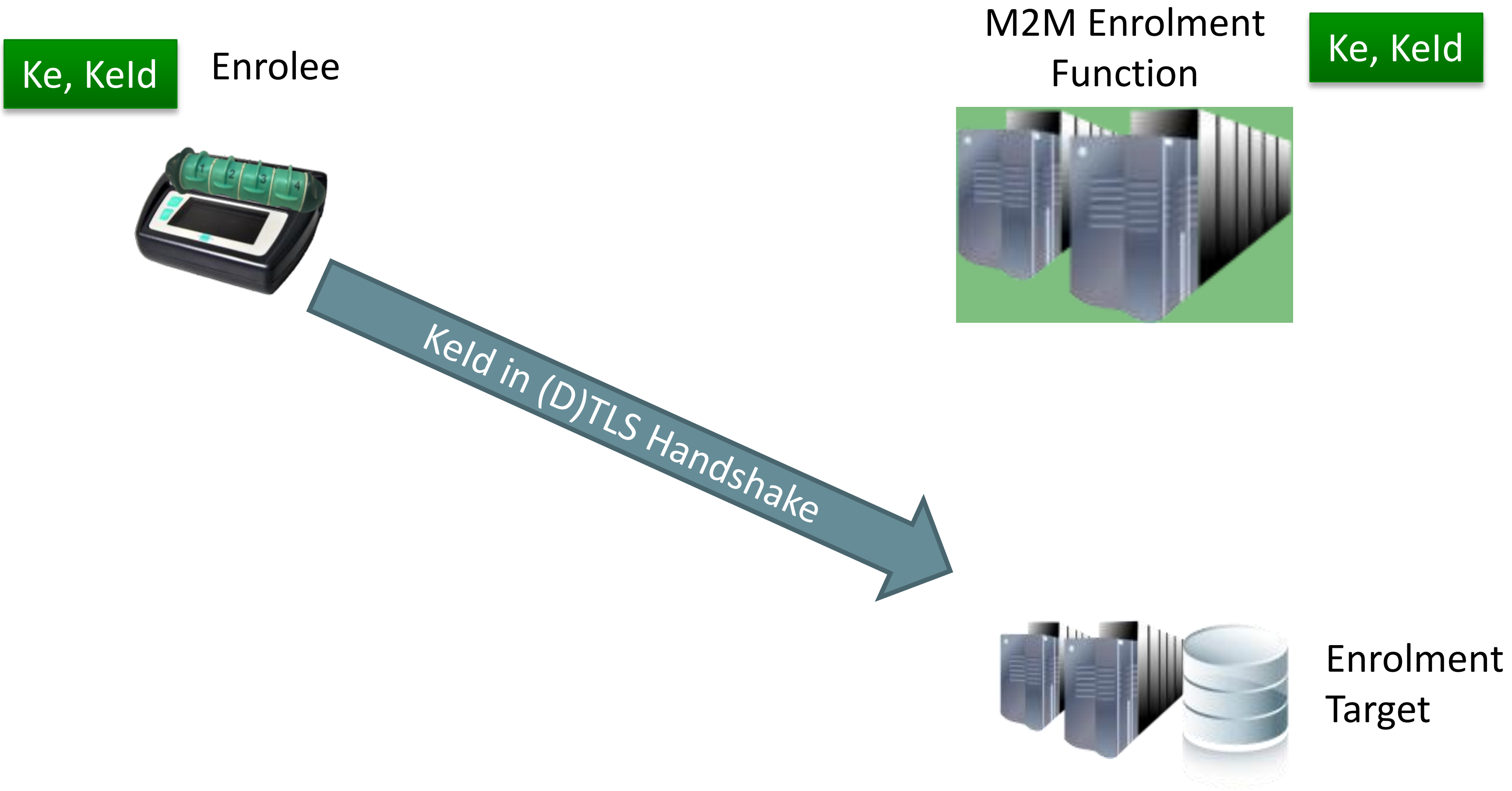
Mutual Authentication

Generate Ke, KeId

Generate Ke, KeId

Enrolment Target

Remote Provisioning



Ke, Keld

Enrolee

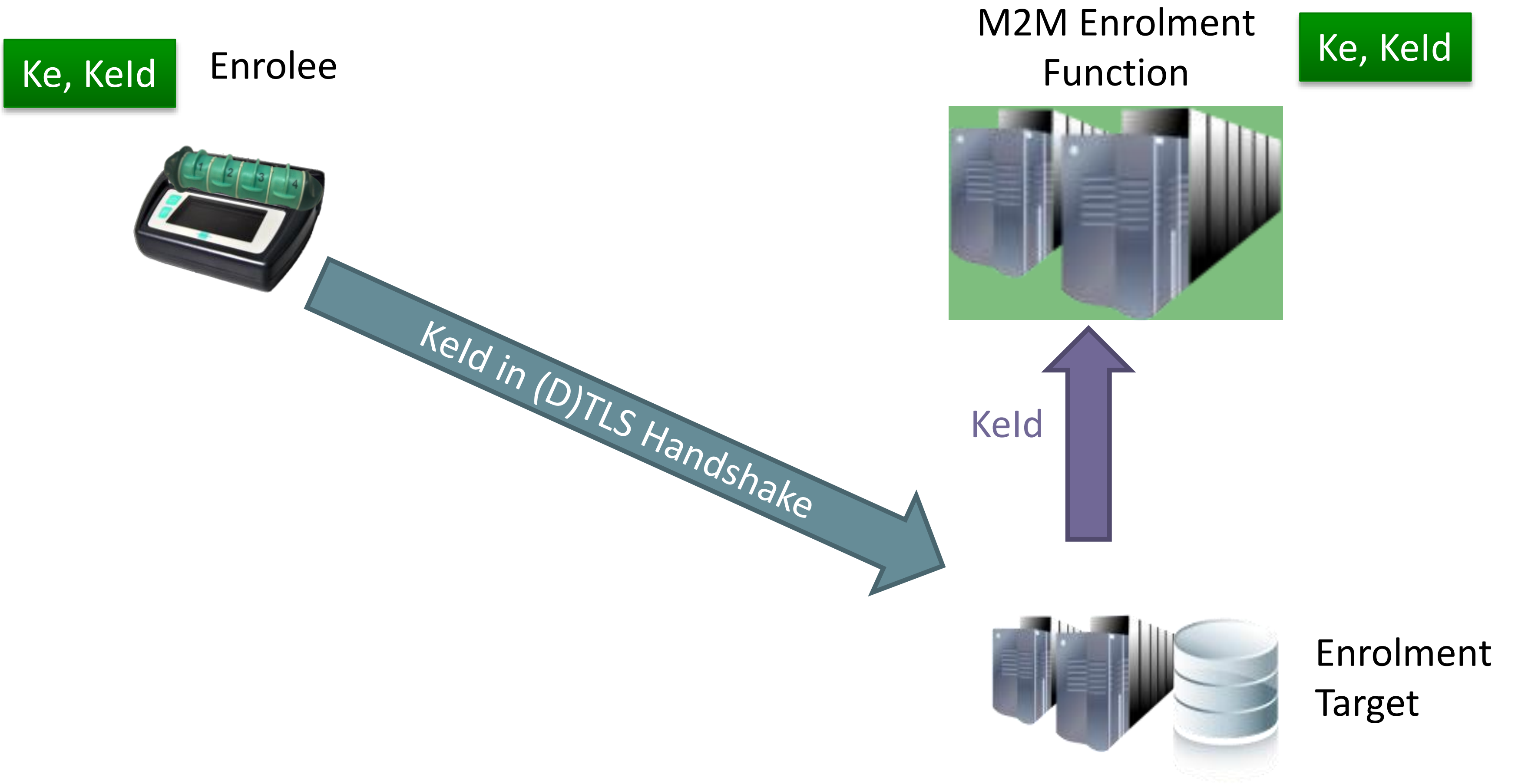
M2M Enrolment Function

Ke, Keld

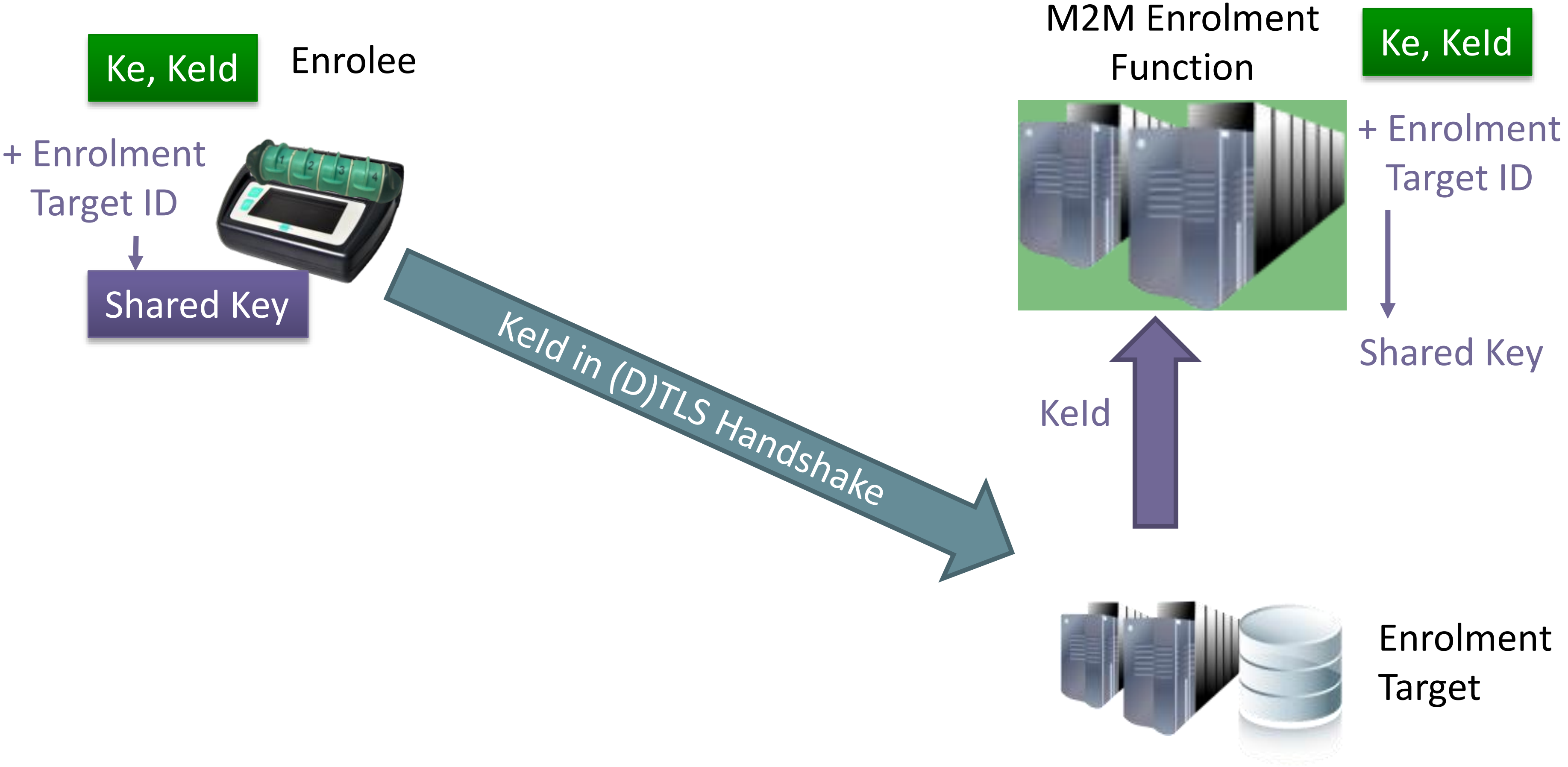
Keld in (D)TLS Handshake

Enrolment Target

Remote Provisioning



Remote Provisioning



Ke, KeId

Enrolee

+ Enrolment Target ID

Shared Key

KeId in (D)TLS Handshake

M2M Enrolment Function

Ke, KeId

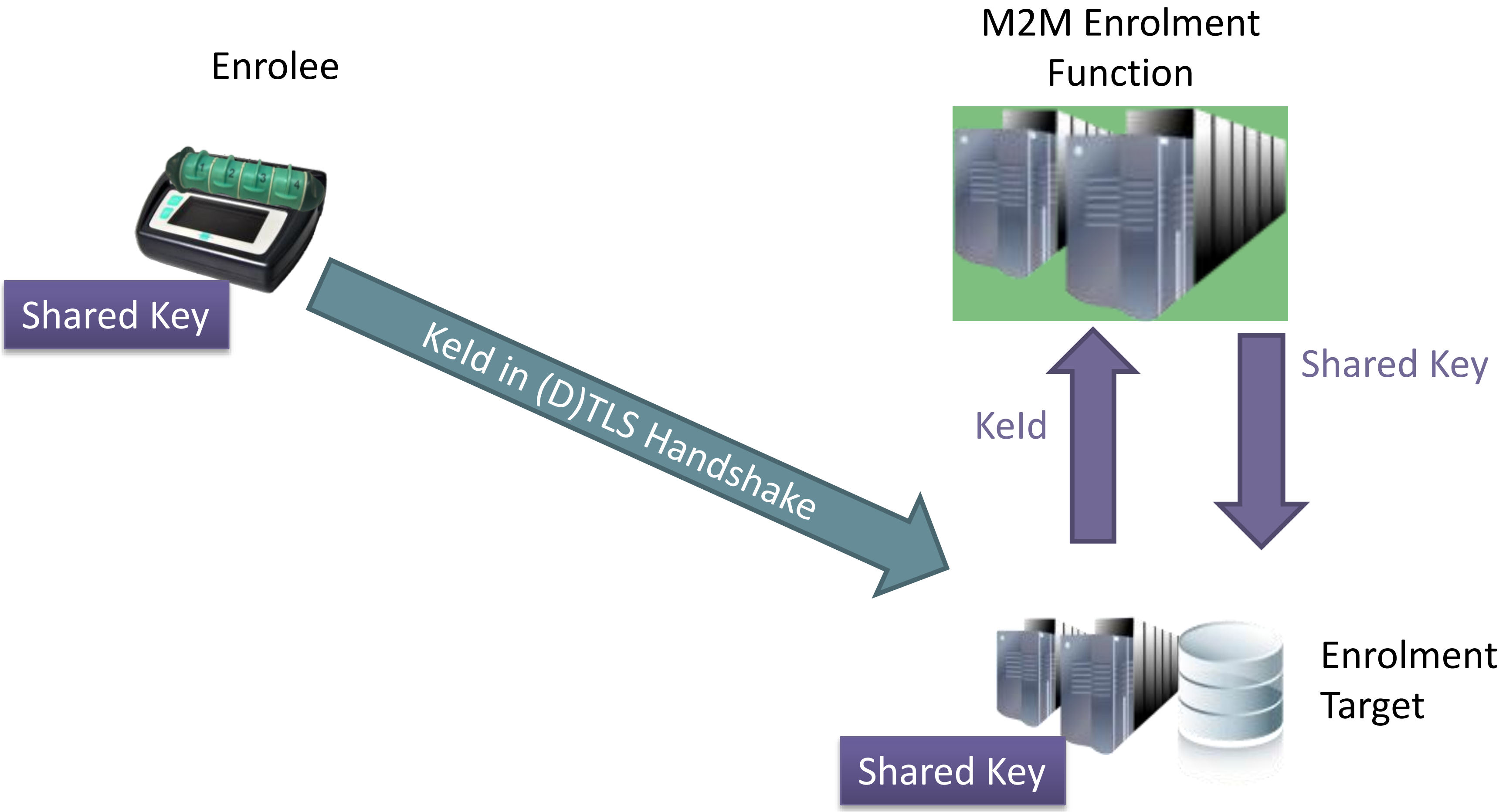
+ Enrolment Target ID

Shared Key

KeId

Enrolment Target

Remote Provisioning



Enrolee

Shared Key

Keld in (D)TLS Handshake

M2M Enrolment Function

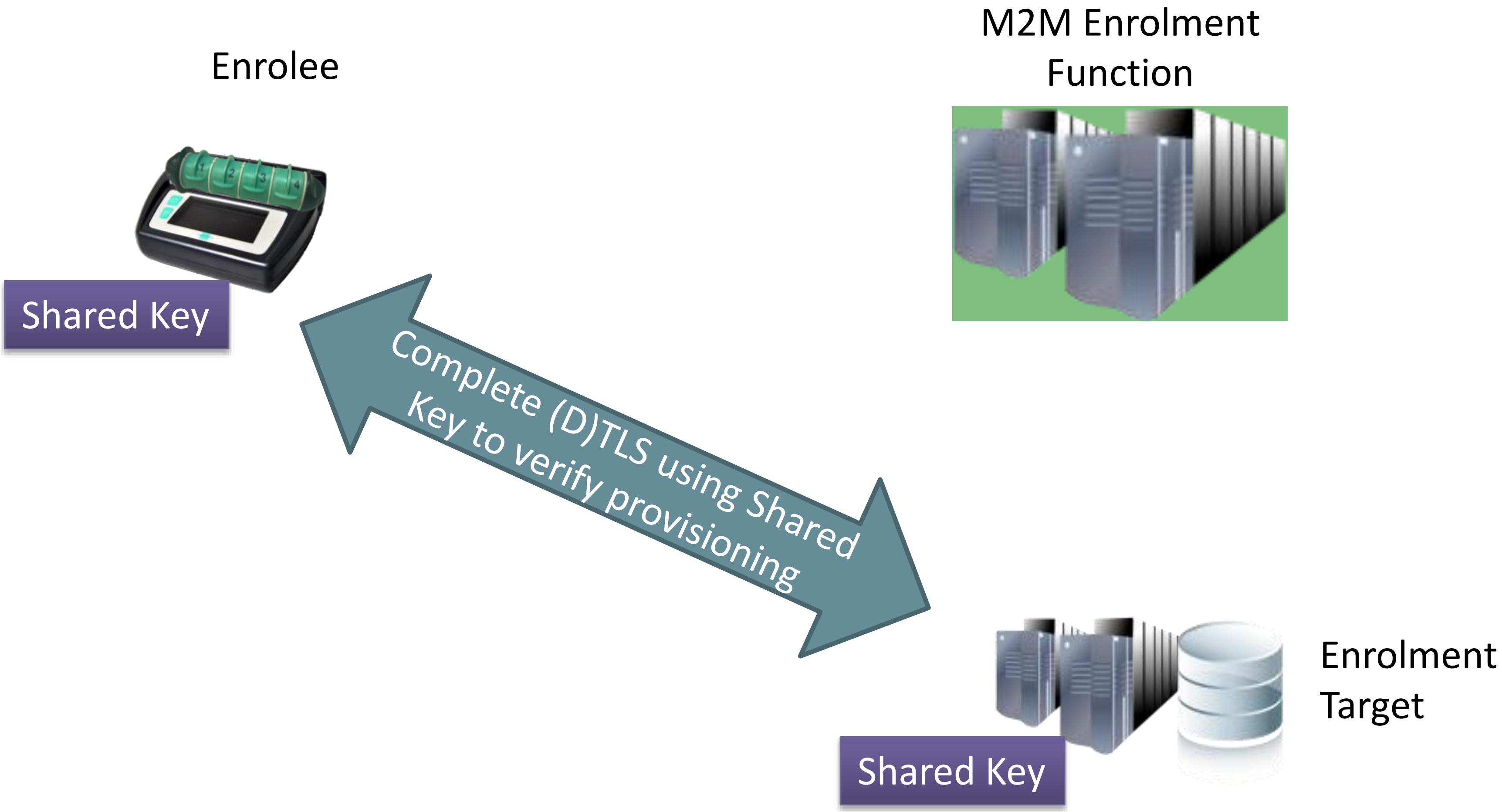
Keld

Shared Key

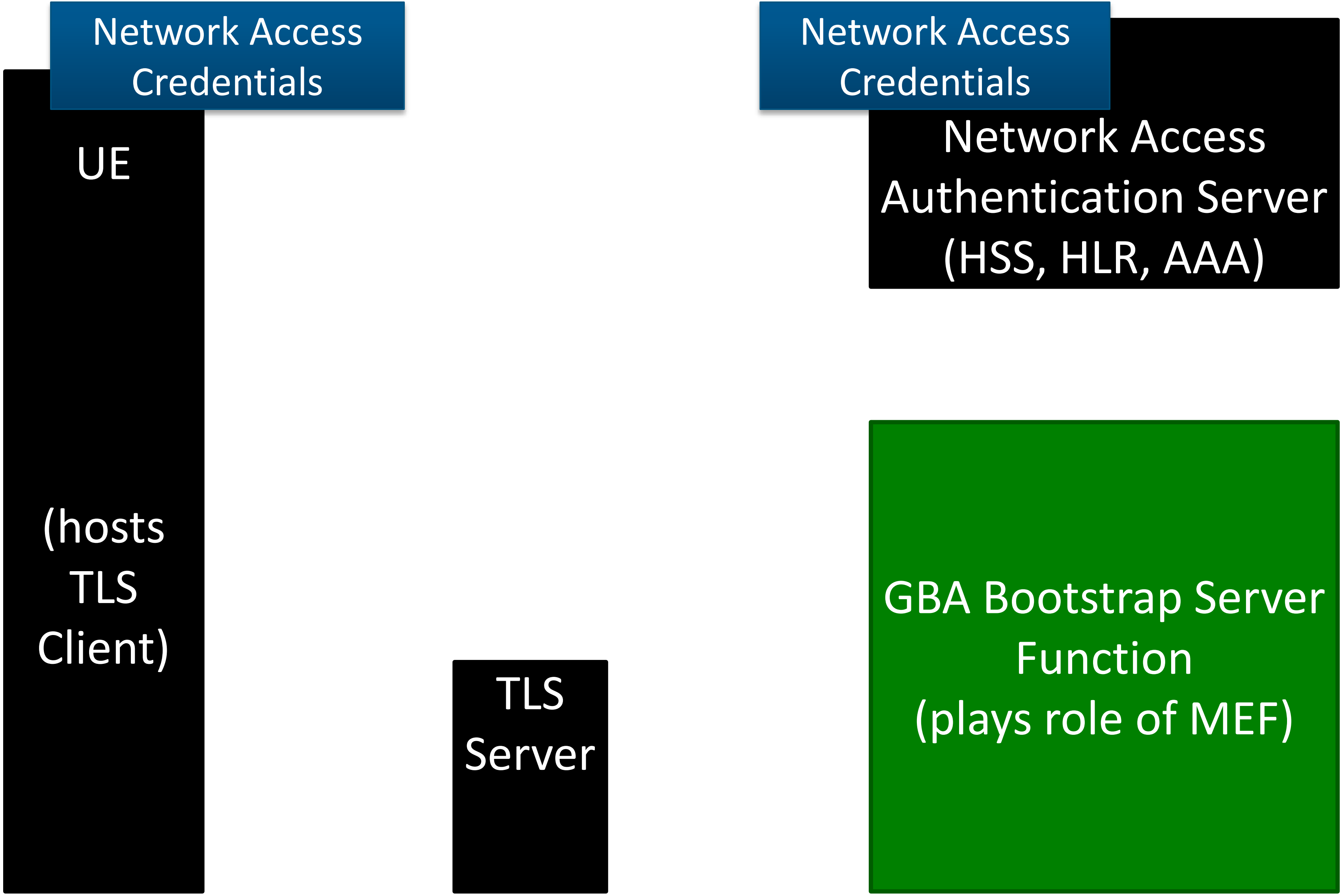
Enrolment Target

Shared Key

Remote Provisioning



GBA



Network Access Credentials

UE

(hosts TLS Client)

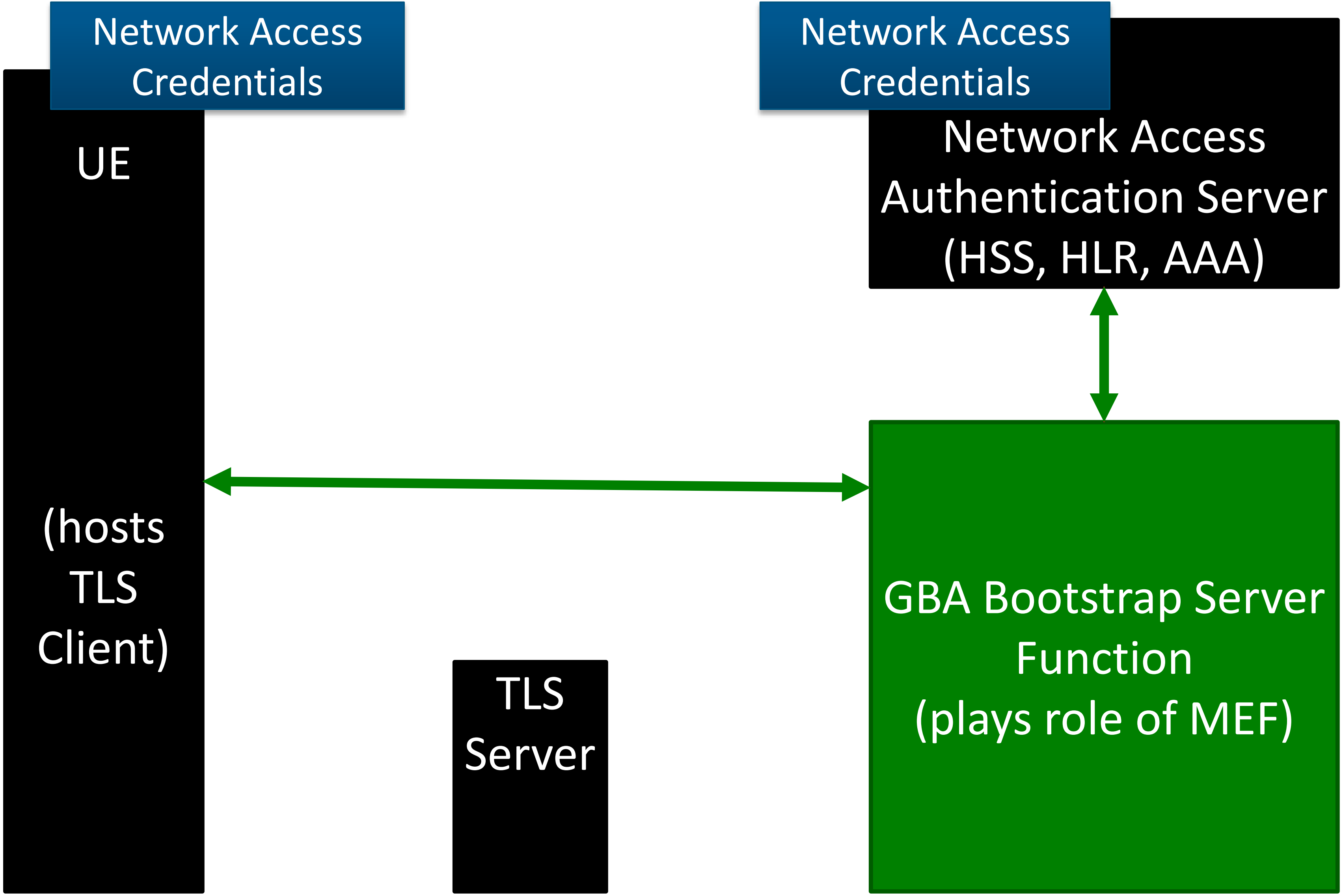
TLS Server

Network Access Credentials

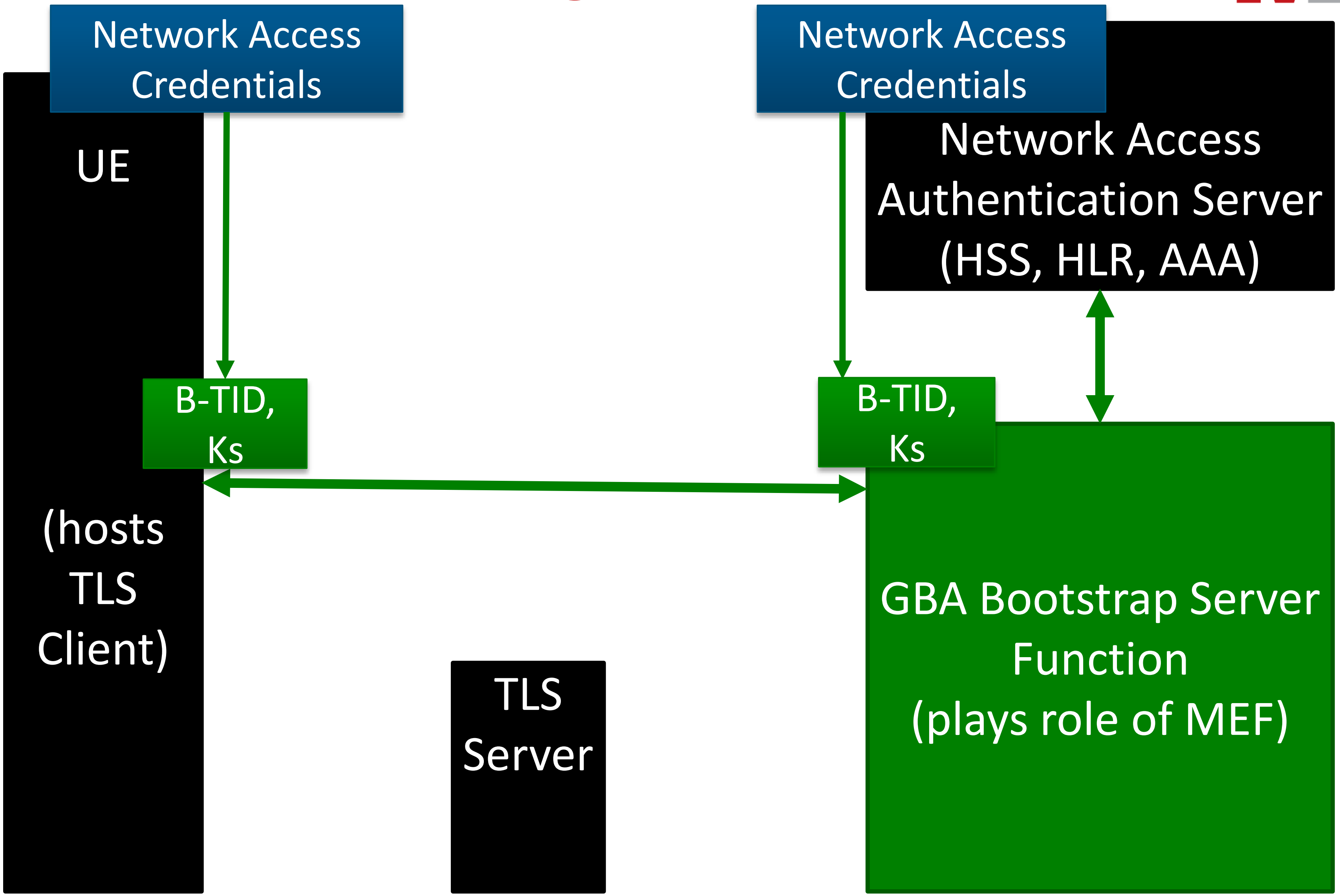
Network Access Authentication Server (HSS, HLR, AAA)

GBA Bootstrap Server Function (plays role of MEF)

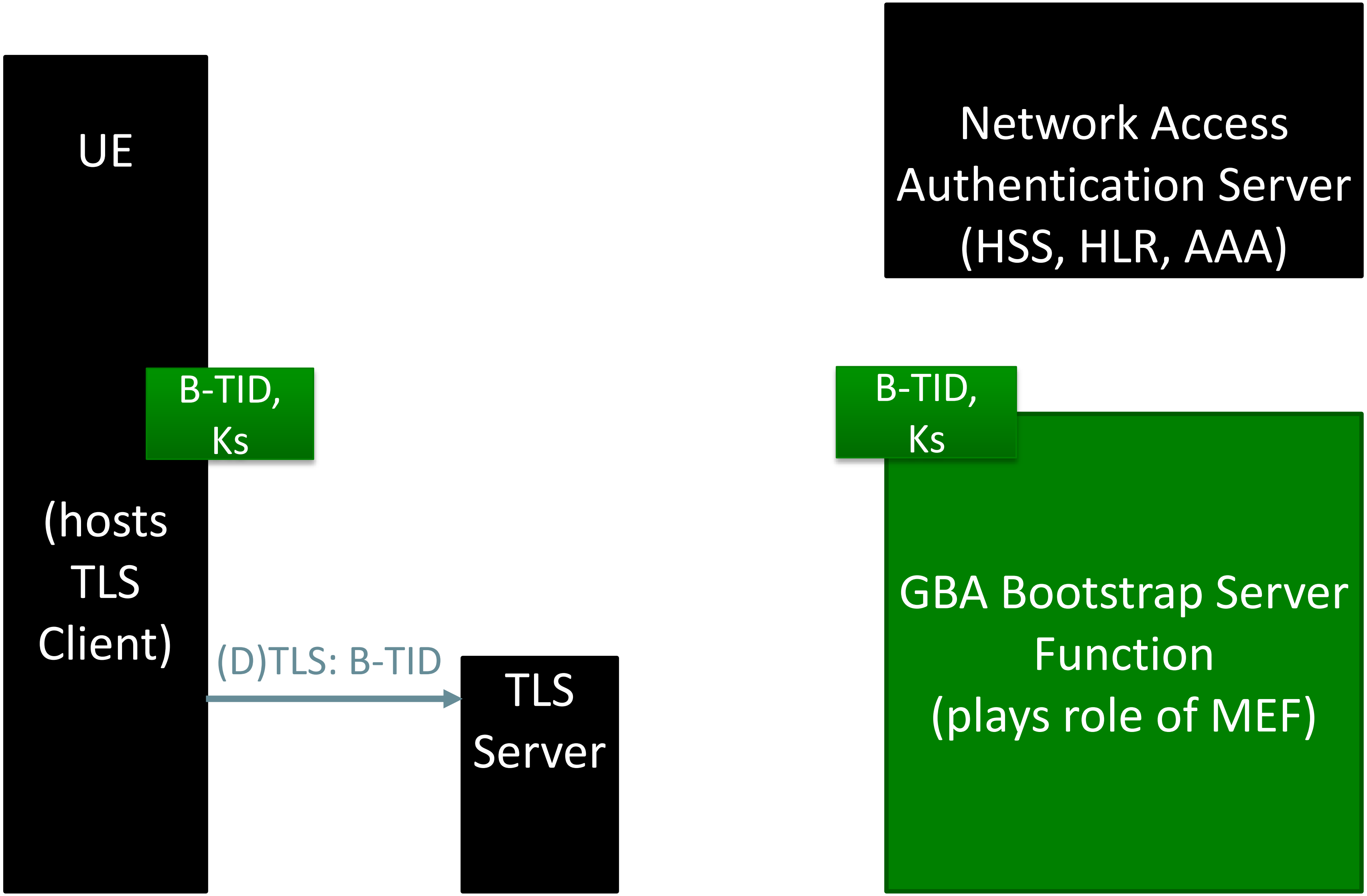
GBA


Network Access Credentials
UE
(hosts TLS Client)
Network Access Credentials
Network Access Authentication Server (HSS, HLR, AAA)
TLS Server
GBA Bootstrap Server Function
(plays role of MEF)

GBA


Network Access Credentials
UE
B-TID, Ks
(hosts TLS Client)
TLS Server
Network Access Credentials
Network Access Authentication Server (HSS, HLR, AAA)
B-TID, Ks
GBA Bootstrap Server Function (plays role of MEF)

GBA



UE

(hosts TLS Client)

B-TID, Ks

(D)TLS: B-TID

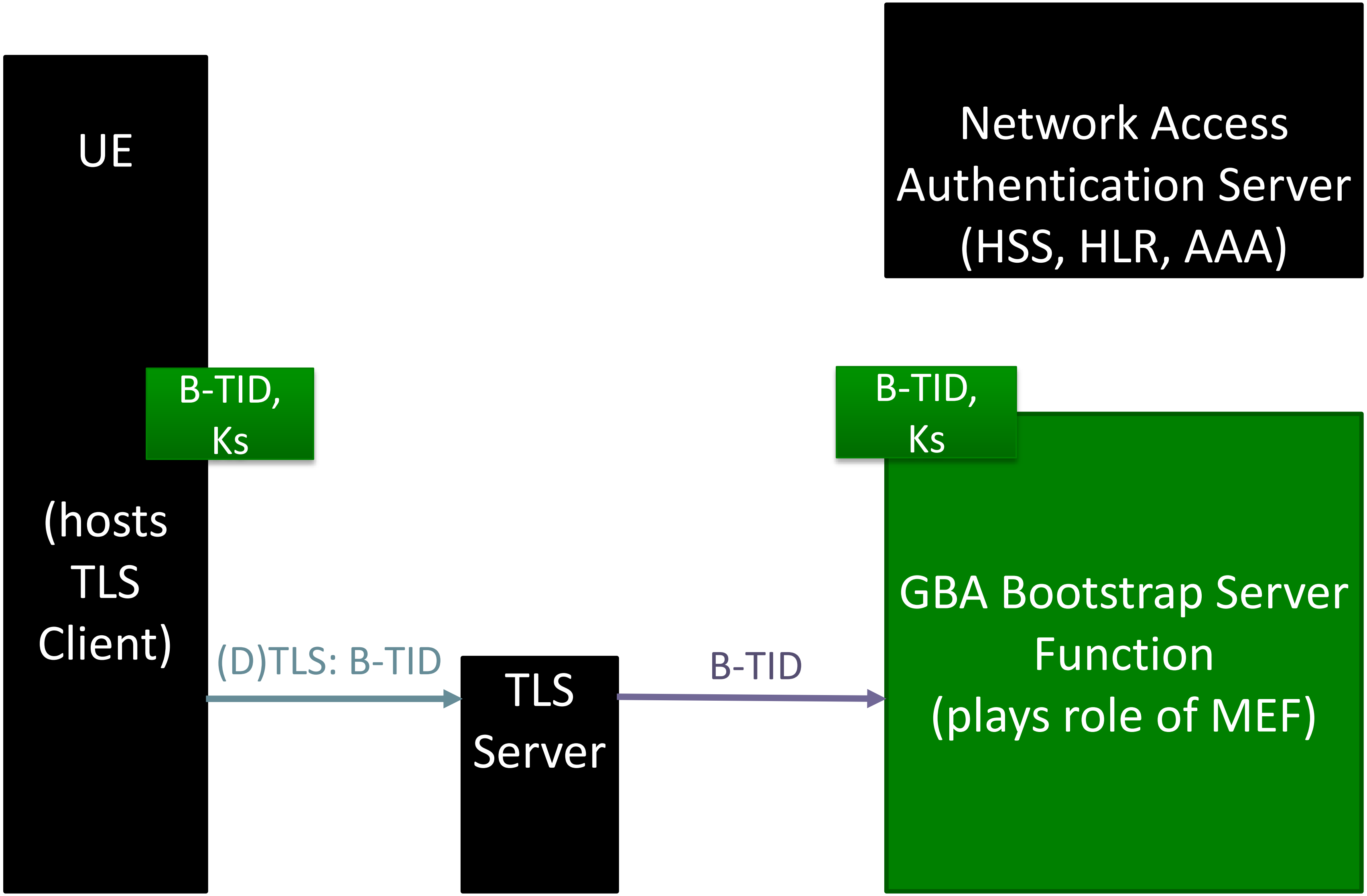
TLS Server

Network Access Authentication Server (HSS, HLR, AAA)

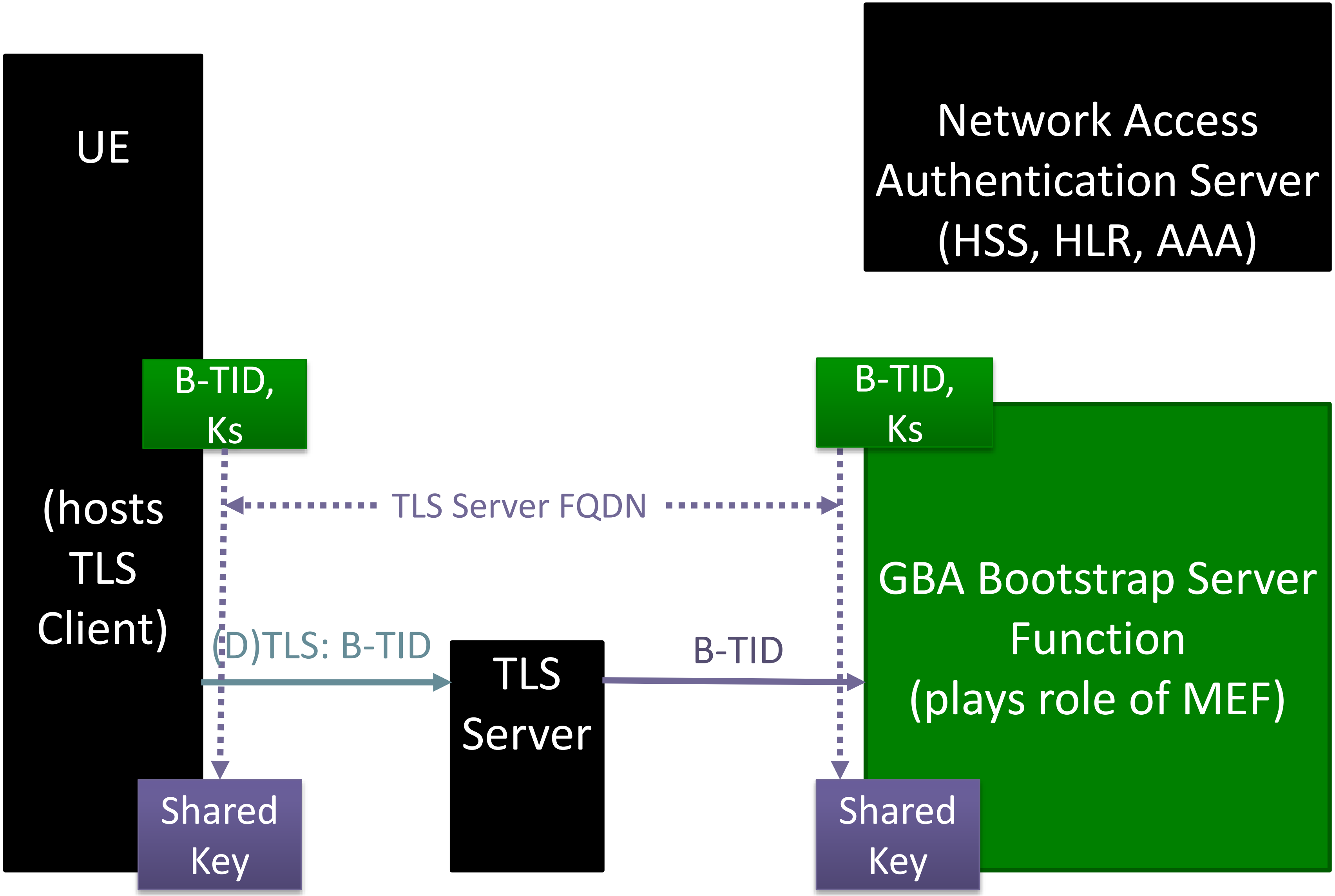
B-TID, Ks

GBA Bootstrap Server Function (plays role of MEF)

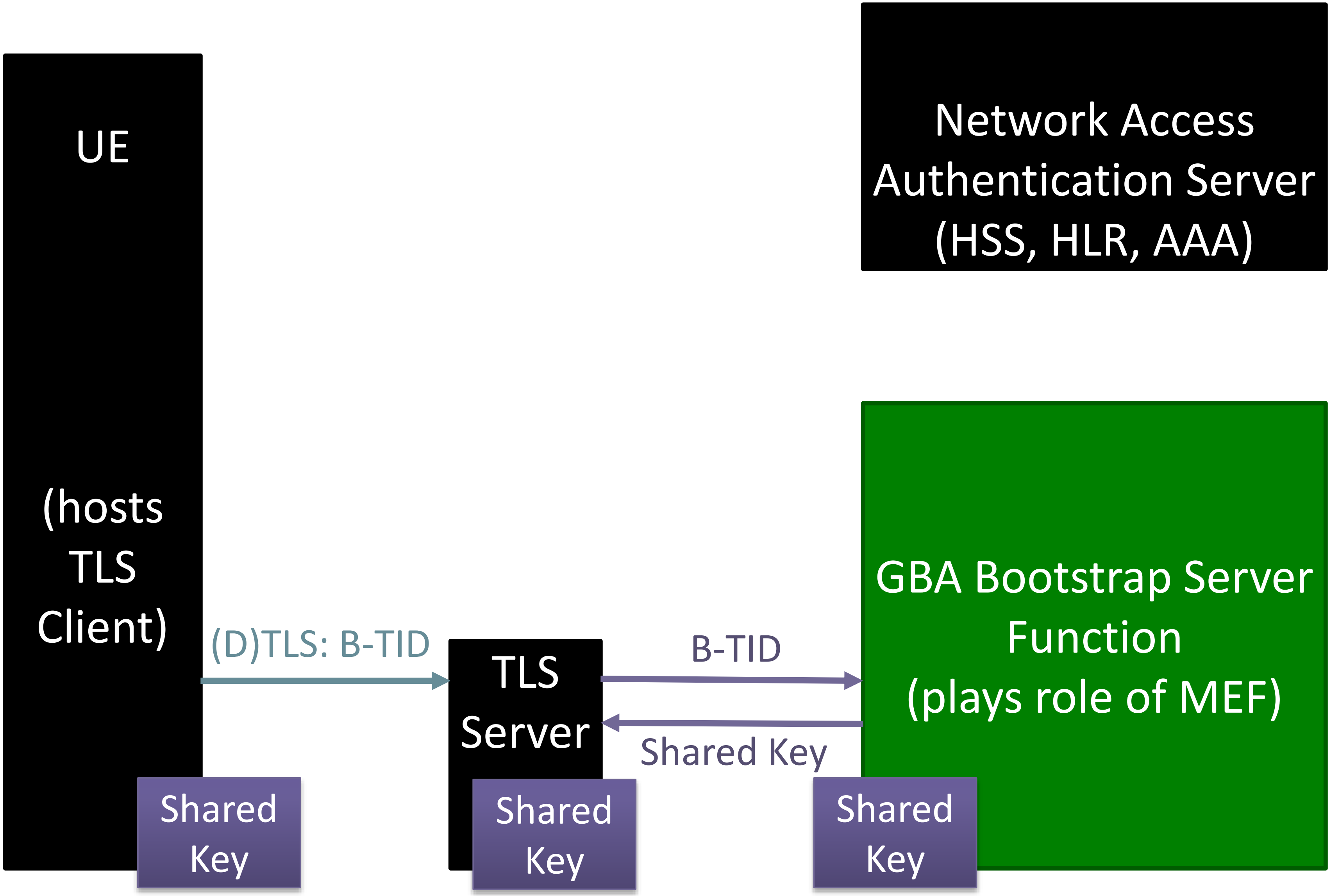
GBA


Network Access Authentication Server (HSS, HLR, AAA)
UE
B-TID, Ks
B-TID, Ks
(hosts TLS Client)
(D)TLS: B-TID
TLS Server
B-TID
GBA Bootstrap Server Function (plays role of MEF)

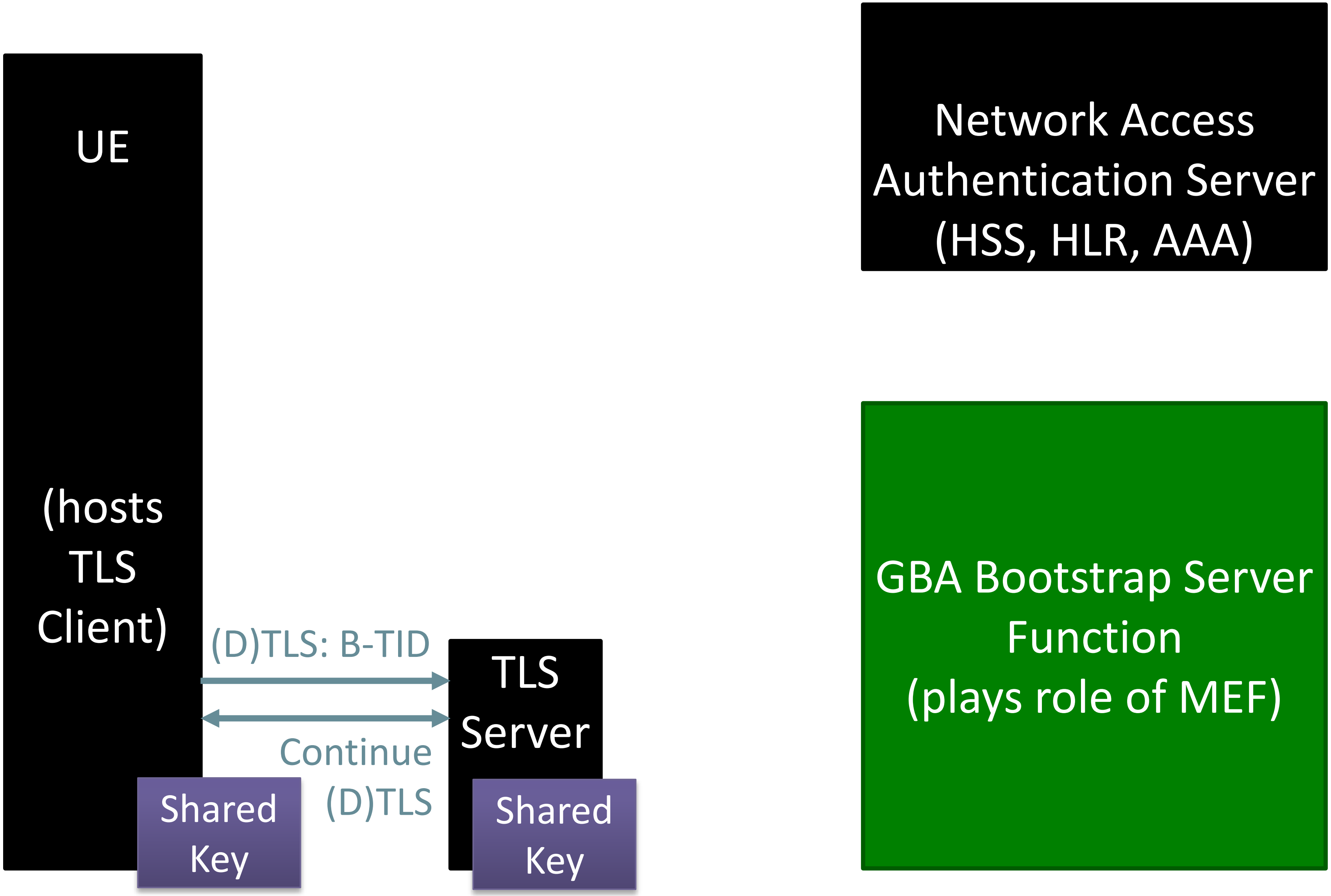
GBA


UE
(hosts TLS Client)
Network Access Authentication Server (HSS, HLR, AAA)
B-TID, Ks
B-TID, Ks
TLS Server FQDN
(D)TLS: B-TID
TLS Server
B-TID
GBA Bootstrap Server Function (plays role of MEF)
Shared Key
Shared Key

GBA


UE
(hosts TLS Client)
Shared Key
(D)TLS: B-TID
TLS Server
Shared Key
B-TID
Shared Key
Network Access Authentication Server (HSS, HLR, AAA)
GBA Bootstrap Server Function
(plays role of MEF)
Shared Key

GBA


UE
(hosts TLS Client)
(D)TLS: B-TID
Continue (D)TLS
Shared Key
TLS Server
Shared Key
Network Access Authentication Server (HSS, HLR, AAA)
GBA Bootstrap Server Function (plays role of MEF)