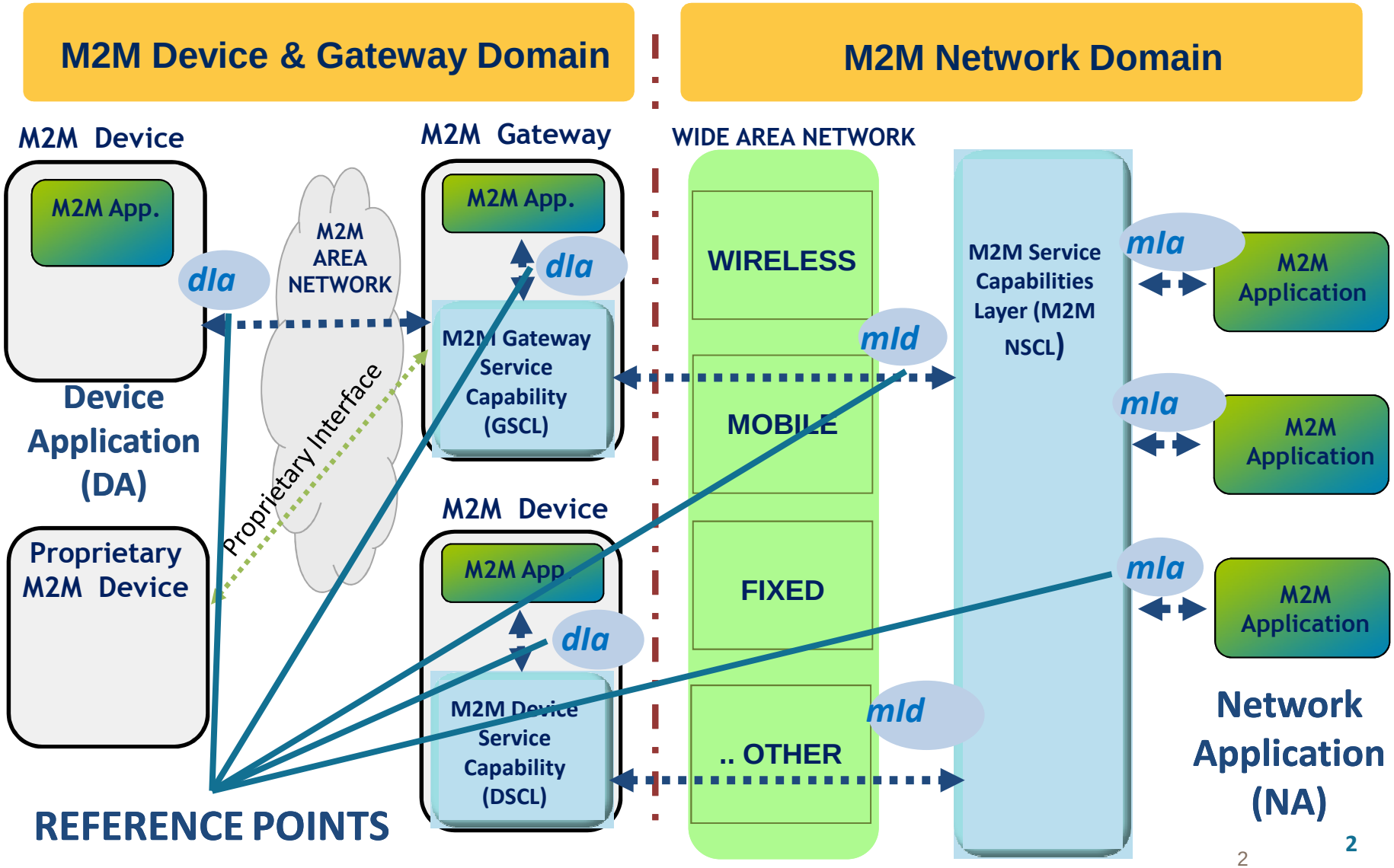
Presentation of ETSI TC M2M security features

ETSI / ISO SC 27 Security Workshop

Source: Francois Ennesser, Security WG chair for ETSI TC M2M and oneM2M

Meeting Date: 2013-04-26

High Level ETSI M2M Architecture



2

ETSI TC M2M, oneM2M and more

- Since 2008, *ETSI TC M2M* develops horizontal services common to multiple M2M applications (energy, transport, healthcare etc.)
- Release 1 published 2011, Rel. 2 being finalized
- Specifications work now migrating to "*oneM2M*" International Partnership of 7 regional telecom SDOs: ETSI, TIA, ATIS, ARIB, TTC, TTA, CCSA
- ETSI TC "*M2M Smart Systems and Services*" remains ETSI leading's committee for related EU mandates, especially M/441 and M/490.

ETSI M2M architecture principles

- ETSI M2M adopted a RESTful architecture style
  - Information represented by resources structured as a tree
- ETSI M2M standardizes resource structure that resides on an M2M Service Capability Layer (SCL)
  - Each SCL contains a resource structure where the information is kept
- M2M Application and/or M2M Service Capability Layer exchange information by means of these resources over the defined reference points
- ETSI M2M standardizes the procedure for handling the resources

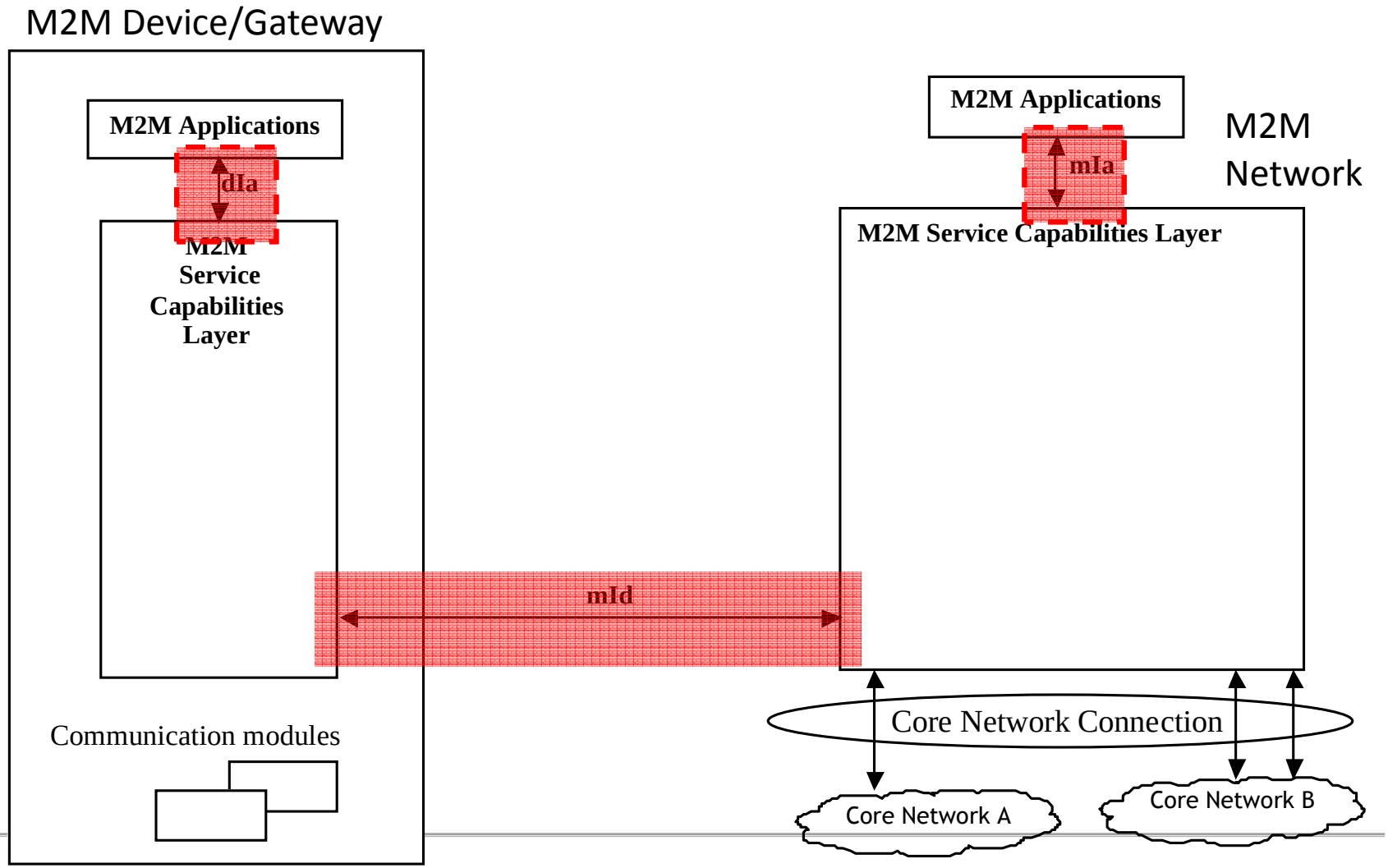
ETSI M2M Security features

- Identification of the M2M Application and the M2M Devices
- Mutual authentication between Network Service Capability Layer and Device/Gateway Service Capability Layer that are connected
- Secure channel for transporting data over mId reference point
- Device/Gateway Integrity validation at Bootstrap and Service Connection

However due to schedule constraints, some security aspects remain unaddressed

- Security mainly addressed for M2M communication Service Providers ("M2M SP")
  - No disociation between "routing" and "trust" based roles in service layer
- Security not addressed "end-to-end"
  - No end-to-end security services offered to applications by service layer

ETSI TC M2M Framework

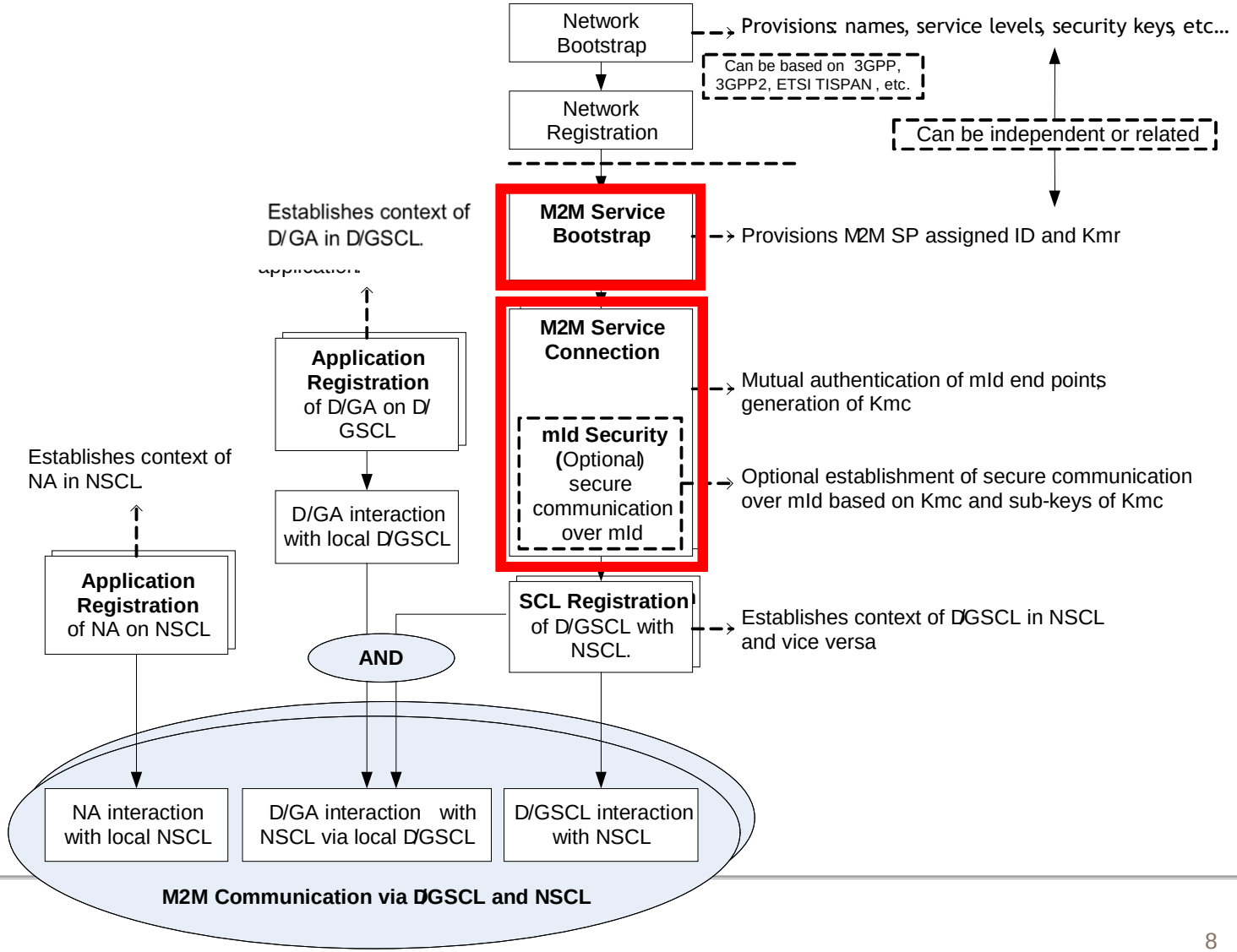


Security has not been addressed

ETSI M2M Security

- ETSI M2M provides standardized security mechanisms for the reference point *mId*
- Devices/gateways hold secret keys protecting the connection in a *"secured environment"*
- The device/gateway is provisioned with the key *M2M Root Key.*
- The high level procedure are to
  - Perform mutual *mId* end point authentication
  - Perform *M2M Service Connection Key* agreement
  - Optionally, establish a secure session over *mId*.
  - Perform RESTful operations over *mId*

M2M Service Layer Procedures

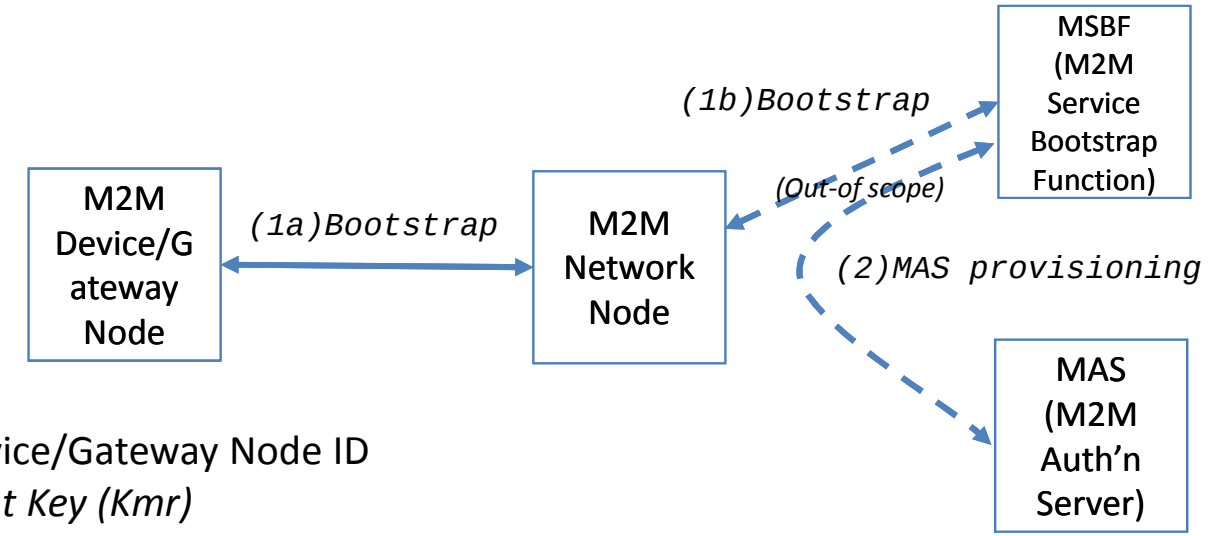


Service Bootstrap Procedures

- Access network (AN) dependent vs. access-agnostic bootstrap
  - May derive M2M service credentials from existing AN credentials (e.g. UICC based)
  - Or provide independent service layer credentials
- Bootstrapping of M2M Service Layer Credentials on the field:
  - Establishment of shared secret Kmr in Device and Network over mId
  - Pre-provisioning (e.g. Smartcard based) or Automated (infrastructure assisted) methods
- Automated bootstrap procedures
  - GBA: NAF serves as MSBF (M2M Service Bootstrap Function)
    - Uses Access Network credentials in UICC (e.g. USIM, CSIM or ISIM application)
    - Uses same HTTP procedure as TLS/TCP for bootstrap parameters delivery
  - EAP/PANA: Dedicated MSBF + MAS (M2M Authentication Server)
    - Uses any type of credentials (SIM, AKA, PSK, certificates, IBE, OTP, etc.)
    - Access Network based: e.g. UICC with EAP-AKA / Kmr based on EMSK
    - Or Access-agnostic: EAP-IBAKE, or EAP-TLS with certificates
  - TLS/TCP (Access agnostic)
    - Uses X.509 certificates pre-provisioned on the device/gateway
    - 256 bits encr. key, TLS 1.2 RSA AES 128 CCM or TLS 1.1 RSA AES 128 CBC SHA
    - AES 256 Key Wrap

Generic Bootstrap Procedure

Input:
- Pre-provisioned device/gateway ID
- *Pre-provisioned secret key*



Output:
- M2M Device/Gateway Node ID
- *M2M Root Key (Kmr)*
- Lifetime
- Optionally:
  - D/GSCL-ID
  - NSCL-ID

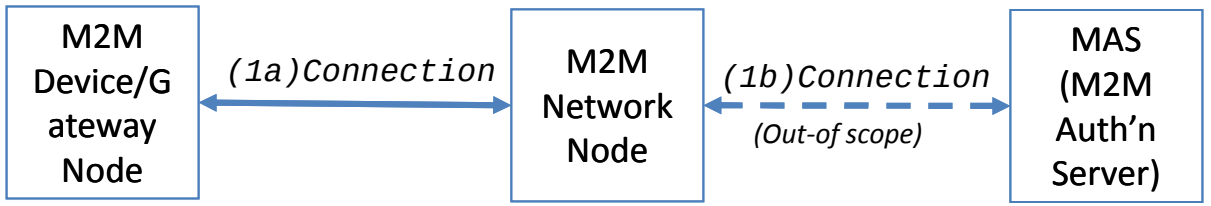
Service Connection Procedures

- Optional derivation of M2M Service Connection (session) Key *Kmc*
  - Not needed (i.e., no Kmc) when relying on existing access network security
- Access Network dependent vs. access-agnostic
  - Direct derivation from existing AN credentials (e.g. in UICC based AN subscription) possible for GBA and EAP (no Kmr)

- Connection procedures
  - GBA (access dependent Kmc)
    - Uses Access Network credentials in UICC (e.g. USIM, CSIM or ISIM application)
  - EAP/PANA
    - Uses xSIM/UICC with EAP-SIM/EAP-AKA (access-dependent Kmc), or
    - Uses Kmr as PSK with EAP-GPSK (access-agnostic), or
  - TLS/TCP (access agnostic, uses Kmr as PSK)
    - TLS 1.1 or 1.2 with ECDHE PSK AES 128 CBC SHA (256)

Generic Connection Procedure

Input:
- M2M Device/Gateway Node ID
- *M2M Root Key*

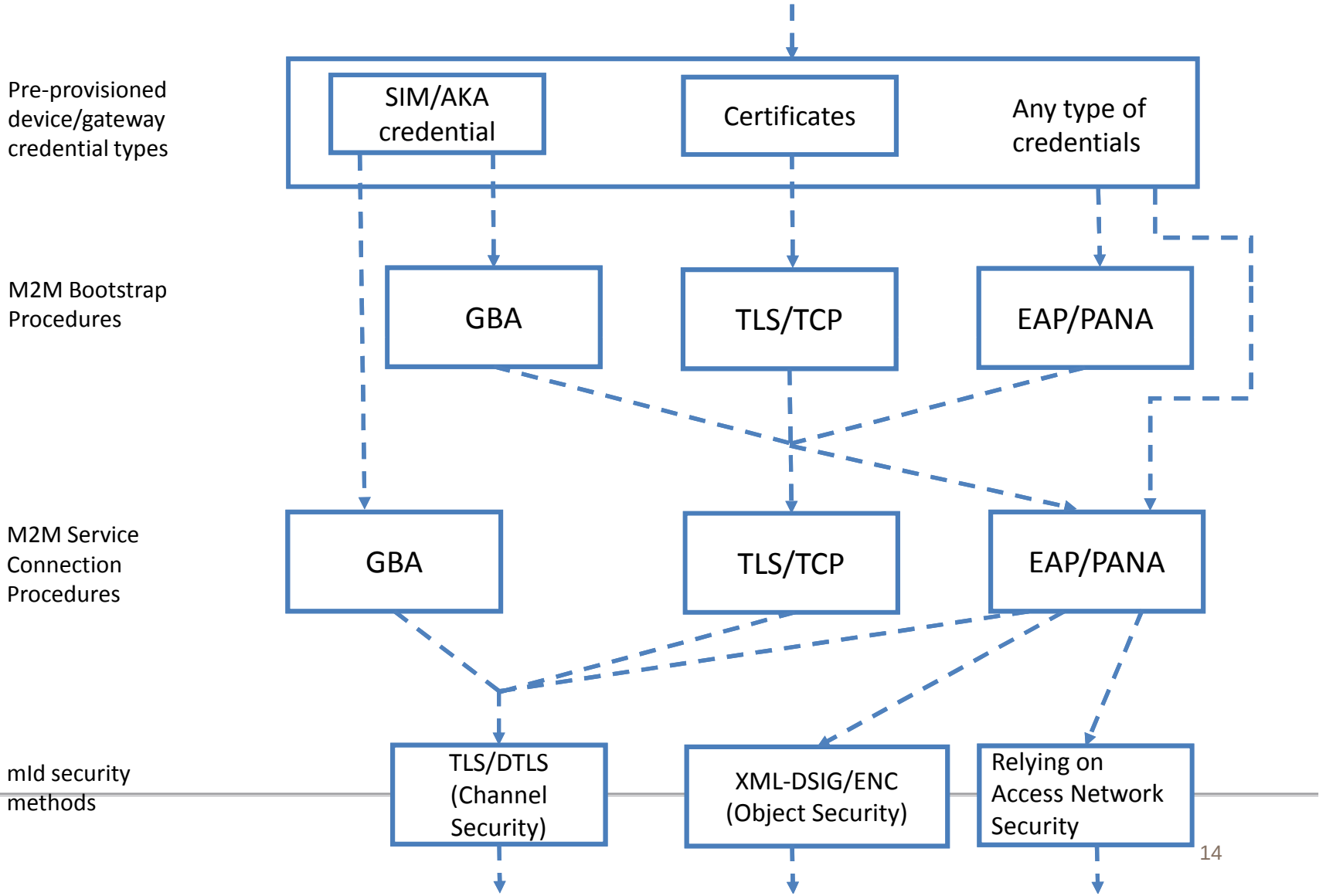


Output:
- M2M Connection ID
- *M2M Service Connection Key (Kmc)*
- Lifetime
- mId security method/parameters
- Optionally:
  - D/GSCL-ID

Secure connection (mId Interface)

- One or more of the following methods used
  1. Relying on a trusted access network (i.e., lower-layer) for security
     - This is the case where no Kmc is derived
  2. Using **channel security** (PSK AES 128)
     - HTTP: TLS/TCP, TLS 1.2 CBC SHA or TLS 1.1 CCM
     - CoAP: DTLS/UDP , DTLS 1.2 CCM(_8)
  3. Using **object security** (lacks interoperable flexibility in current releases)
     - XML-DSIG and XML-ENC (v 1.1), using Kmc

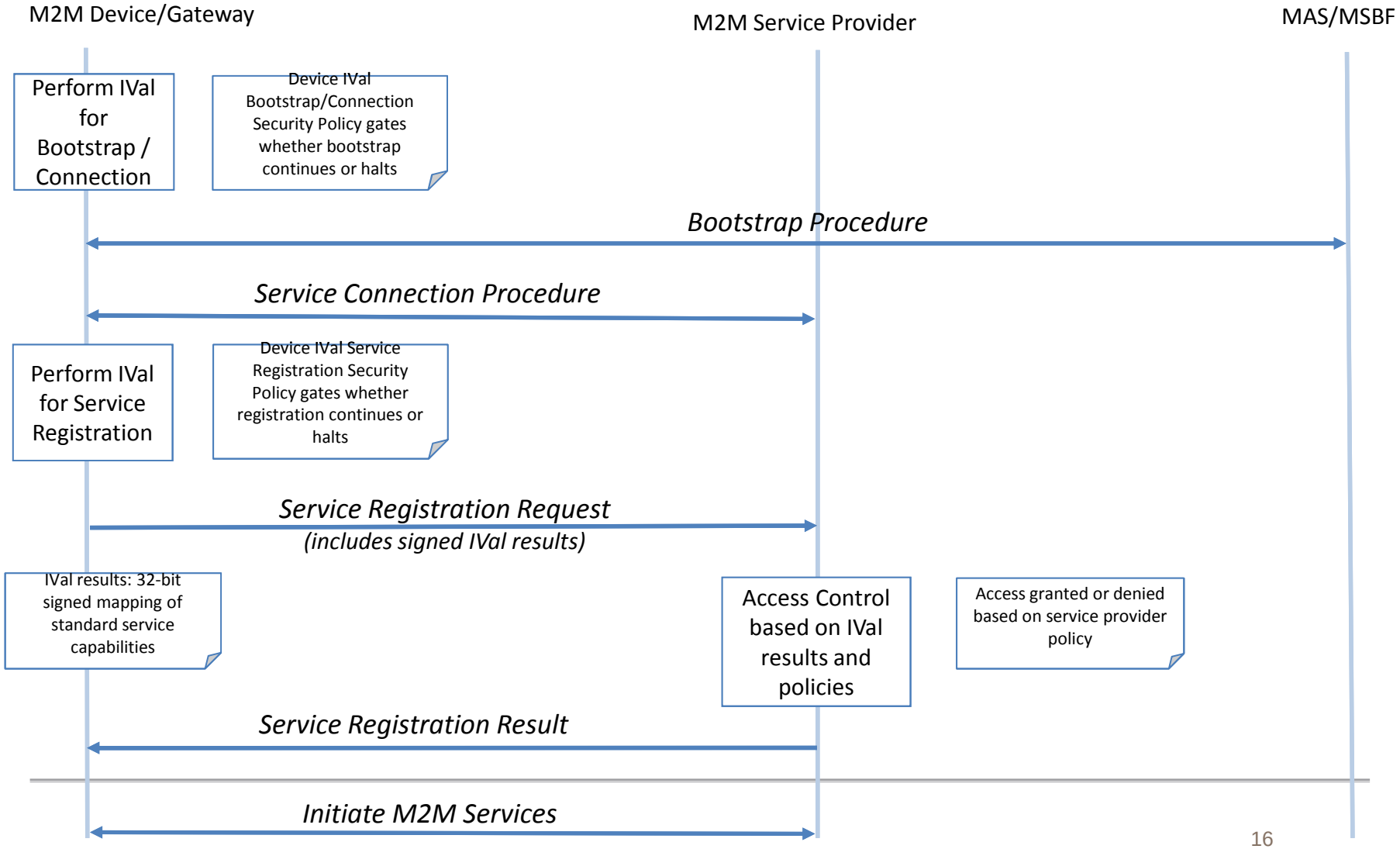
Security Scenarios - Baseline



ETSI Support of Integrity Validation

- Integrity Validation (IVal)
  - optional feature enabling e.g. to detect tampering of device
  - enables fine grained access control for both M2M Device/Gateways and M2M Service Providers.
- Rel-1 supports IVal prior to Bootstrap and during Service Registration procedures
  - Code Integrity checks performed/stored in Secured Environment
  - IVal result (4 bytes):
    - Mapping device software image to standard M2M services
    - Sent to M2M Service Provider during service registration.
    - Signed with IVal key to ensure integrity and authenticity of reported results.
  - The M2M Service Provider can grant or deny service access based on the reported IVal results and provider policy

Integrity Validation Call Flow



Contact Details:

francois.ennesser@gemalto.com

Thank you!