## Types of Devices and Network Structure

There are three roles a participant can act as:

• Border Router

• Commissioner

• End Device

## Definitions:

### Border Router

Any device capable of forwarding between a Mesh Network and a non-Mesh Network. The Border Router also serves as an interface point for the Commissioner when the Commissioner is on a non-Mesh Network. The Border Router requires a Mesh interface.

### Commissioner

The authentication server for new Devices and the authorizer for providing the Network Credentials they require to join the network. A device capable of being elected as a Commissioner is called a Commissioner Candidate. Devices without mesh network interfaces may perform this role. This device may be, for example, a cell phone or a server in the cloud, and typically provides the interface by which a human administrator manages joining a new device to the Thread Network.

### Commissioner Candidate

A device that is capable of becoming the Commissioner, and either intends or is currently petitioning the Border Router to

become the Commissioner, but has not yet been formally assigned the role of Commissioner.

### Commissioning Credential

A human-scaled passphrase for use in authenticating that a device may petition to become the Commissioner of the network. This passphrase is encoded in utf-8 format and has a length of six (6) bytes minimum and 255 bytes maximum. This credential can be thought of as the network administrator password for a Thread Network.

The first device in a network, typically the Border Router, MUST be out-of-band commissioned to inject the correct user generated Commissioning Credential into the Thread Network, or provide a known default Commissioning Credential to be changed later. This credential is used to derive an enhanced key using key stretching called the PSKc (Pre-Shared Key for the Commissioner) which is used to establish the Commissioner Session.

### Commissioning Key (PSKc)

The PSKc (Pre-Shared Key for the Commissioner) is a derived key based on the Commissioning Credential which is used to establish the Commissioner Session. The PSKc is used as a passphrase input to a PAKE cipher suite, such as J-PAKE [draft-hao-jpake-03], to establish a secure session between the Commissioner and Border Agent. All devices in a mesh Network will store the PSKc.

### End Device

A Mesh device that transmits and receives unicast traffic only with a Parent device.

### Frame counter

A value that is incremented with each new secured message and used to detect replayed messages.

### Joiner

The device to be added by a human administrator to a commissioned mesh Network. This role requires a mesh Network interface to operate.

### Joining Device Credential

A human-scaled passphrase for use in authenticating that a new Joiner device is the correct one. This passphrase is used in conjunction with a PAKE cipher suite to establish a secure session between the Commissioner and the Joiner. The Commissioner and the Joiner typically share the Joining Device Credential using some out-of-band mechanism such as scanning a barcode or entering a serial number from the Joiner device label. This credential when specifically encoded in binary is referred to as the PSKd (Pre-Shared Key for the Device). A Joining Device Credential is encoded as uppercase alphanumeric characters (base32-thread: 0-9,A-Y excluding I,O,Q, and Z for readability) with a minimum length of 6 such characters and a maximum length of 32 such characters

### Network Credentials

All the security and operational parameters required for a device to be part of a Thread Network as contained in the Joiner Entrust message, including the Network Master Key, Mesh Local Prefix, etc. All devices on a Thread Network store the Network Credentials, including the Leader, Routers, and End Devices

### Server

A device that provides one or more services to a network. Border Routers are considered servers that provide a routing service.

The main goal of the protocol is to authenticate that the correct device is joined, and then to securely transfer the Network Credentials to that device over an unsecured link (secured only by DTLS).

## Commissioner

### Commissioner Authentication

The Commissioner Candidate, after having discovered the Mesh Network of interest, would then securely connect to the Thread Network using the Commissioning Credential.

The Commissioner Authentication step establishes a secured client/server connection between the Commissioner Candidate and a Border Router via DTLS (Datagram Transport Layer Security, [RFC 6347] or optionally TLS (Transport Layer Security, [RFC 5246]. This secured session is hereby known as the Commissioning Session.

The credential used to establish the Commissioning Session is known as the PSKc and is generated as follows.

### Derivation of PSKc

Because the PSKc is stored by all devices in the Thread Network, a key-stretching algorithm is used to protect the actual user-generated passphrase, or Commissioning Credential, that is used to derive it. A Commissioner will locally generate the PSKc, and only authenticate with the Thread Network using that PSKc. This provides some protection for a user that may reuse the same password across various services. The key stretching uses the [PBKDF2](https://ru.wikipedia.org/wiki/PBKDF2) [RFC 2898], AES-CMAC-PRF-128 [RFC 4615].

PSKc = PBKDF2(

PRF=AES-CMAC-PRF-128,

P=<Commissioning Credential>,

S=”Mesh” || <Network Name>,

c=16384, dkLen=16)

Where the **Network Name** is all characters up to the maximum size or null terminator, and 27 || is the concatenation operator.

### Commissioner Registration

After the Commissioner Authentication is successful, the Commissioner Candidate registers its identity with its Border Router by sending message via the secure Commissioning Session.

Message contains a human-readable string that identifies the Commissioner.

Failed attempts by a Commissioner to establish its authority with a Mesh Network shall be rate-limited to RETRY\_DELAY second between attempts up to RETRY\_COUNT attempts and ATTEMPT\_DELAY seconds between such groups of attempts.

### Commissioning

The commissioning process begins when an off-network or on-mesh commissioning device becomes an active Commissioner for a Mesh Network Partition. There can be only one active Commissioner at a time for a Mesh Network, so the commissioning device petitions the Border Router to become the active Commissioner.

An off-network commissioning device, typically a mobile phone, will generally initiate commissioning by discovering the Mesh Network. The device then sets up a DTLS connection with the Border Agent using the network's Commissioning key (PSKc).

Once active, the Commissioner can enable joining on the network and optionally provide data that indicates the ID of the devices expected to join.

A joining device (Joiner) can then communicate with the Commissioner via a relaying protocol through Border Router to which the Commissioner is connected. The Joiner and the Commissioner then perform a DTLS handshake using the Joiner’s passphrase, which the Commissioner MUST have received out-of-band, typically by being entered by a user. Once the handshake is complete, the shared secret it produces is used to pass the Mesh Network’s commissioning material from the Commissioner (Router in case of OT) to the joining device.

Sending master key from Commissioner is easier than from Router because: 1) protocol is simpler; 2) Commissioner is allowed to obtain master key from Border Router.

The Commissioner may also query and set Mesh Network parameters, such as the Mesh Network name and security configuration (i.e. master key).

The high level view of commissioning-joining procedure is depicted on the UML sequence diagram below:



## Border Router. Role in Commissioning

Border Routers play a role in commissioning of new devices to the Mesh Network. A Border Router implements a commissioning Border Agent which acts as a relay for messages between external Commissioners (such as a mobile device) and devices on the interior network.

Router MUST be specifically provisioned for immunity to Denial of Service (DoS) situations that may be based on generation of multiple requests in their radio vicinity.

Where a random number is required as specified in this document, a device MUST implement a True Random Number Generator (TRNG) where the entropy source can be proven to be from a verifiably random source, e.g., from thermal noise, avalanche noise, or atmospheric noise.

## Joiner

### Joining a Thread Network

To join a mesh Network a device must first acquire the following commissioning information:

*thrKeyRotation*

Key rotation period in hours. The minimum key rotation period SHALL be 1 hour and a key rotation period of 0 SHALL NOT be allowed.

*thrKeySequenceCounter*

Monotonically increasing counter used for key rotation.

• Master Key

• Commissioning Key (PSKc)

• Network Name (used in derivation of PSKc - provides some protection for a user that may reuse the same password across various services.)

These may be obtained either through in-band commissioning or through out-of-band commissioning. Out-of-band commissioning is not defined in this specification, other than a requirement that it be at least as secure as in-band commissioning.

### Joiner Authentication

The Joiner, throughout the Joining process, sends DTLS handshake messages via unsecured channel to a Router. A Router relays these messages on to Commissioner. Any Router has no knowledge of the content of these Joiner messages, and only relay data on the unsecured channel.

## Regular traffic

### Network-wide Key

The Mesh Network is protected with a network-wide key (master key), from which derived key are used (in OT at the MAC sub-layers to protect the 802.15.4 MAC data frames). This is an elementary form of security used to prevent casual eavesdropping and targeted disruption of the Network from outsiders without knowledge of the network-wide key. Because it is a network-wide key, compromise of any Mesh device could potentially reveal the key. (As a result, the network-wide key is not typically used as the only form of protection within the OT Network). From the point of view of joining the network, it is used to discriminate between an authenticated and authorized device and the joining device (in its initial state).

Because the joining device is untrusted at the point of joining, it is common practice to enforce some sort of policing mechanism to ensure the joining device can be verified and at the same time limit the effect of rogue devices attempting to join the Mesh Network. In a Mesh Network, this requires the joining device to identify a trusted device and to communicate solely in a point-to-point fashion with this trusted device. The trusted device polices any traffic from the joining device and forwards it to the commissioning device in a controlled manner to allow the authentication protocol (DTLS handshake) to execute.

In the usual case where the commissioning device is not in direct communication with the joining device, the trusted device MUST relay the DTLS handshake with the commissioning device through one relay agent - Router. A relay protocol provides encapsulation of the DTLS handshake and relaying of the DTLS handshake from the joining device all the way to the commissioning device in a simple manner.

### Master Key

Key used to derive security material for MAC protection in OT. For simplicity in this paper key rotation period and sequence counter (that participate in OT in key derivation) are not used because this would require complex protocol for propagation of counter to network devices – synchronization of counter.

***Not used in this version*** *but used in OT:*

*thrKeyRotation*

Key rotation period in hours. The minimum key rotation period SHALL be 1 hour and a key rotation period of 0 SHALL NOT be allowed.

*thrKeySequenceCounter*

Monotonically increasing counter used for key rotation.

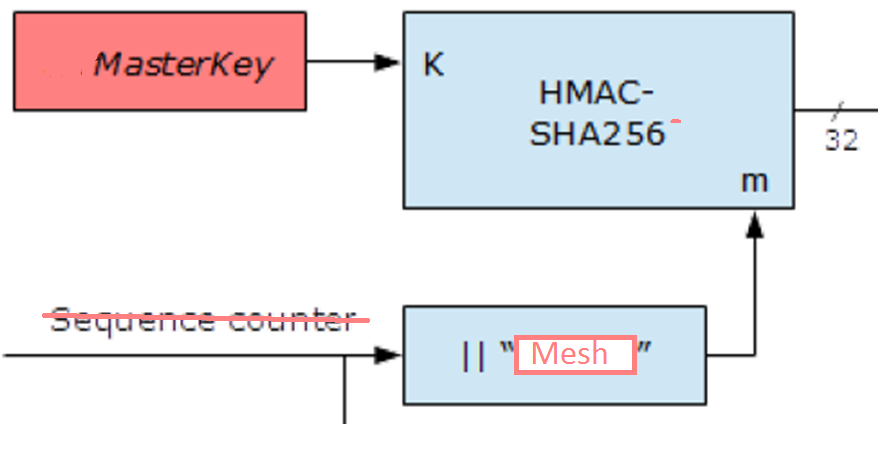
### **Key Generation**

**(**may be omitted if master key is always equal to necessary length for AES cipher**)**

Each Thread node receives the Master Key when joining and assigns it to the *MasterKey* attribute. In OT - *MasterKey* is used in conjunction with a sequence counter to derive two separate keys for use by the MAC sublayer and MLE. **This version** uses key derivation to make **derived master key (DMK) of particular length** (key stretching hash algorithm is used if master key may be of variable length. If master key is equal to length of AES key – then derivation may be omitted. Master key should be generated by Router (not user) therefore master key may be always of the same length). The use of Hashed Message Authentication Mode with the SHA-256 algorithm (HMAC-14 SHA256) as the keyed hash function produces an output of 32 bytes [RFC 6234]. Therefore, DMK, used for encryption of regular traffic maybe up to 32 bytes. The 32-byte DMK key is generated as follows:

HMAC-SHA256(MasterKey, ~~sequence counter ||~~ “Mesh”)

where || is the concatenation operator and “Mesh” is the byte sequence.

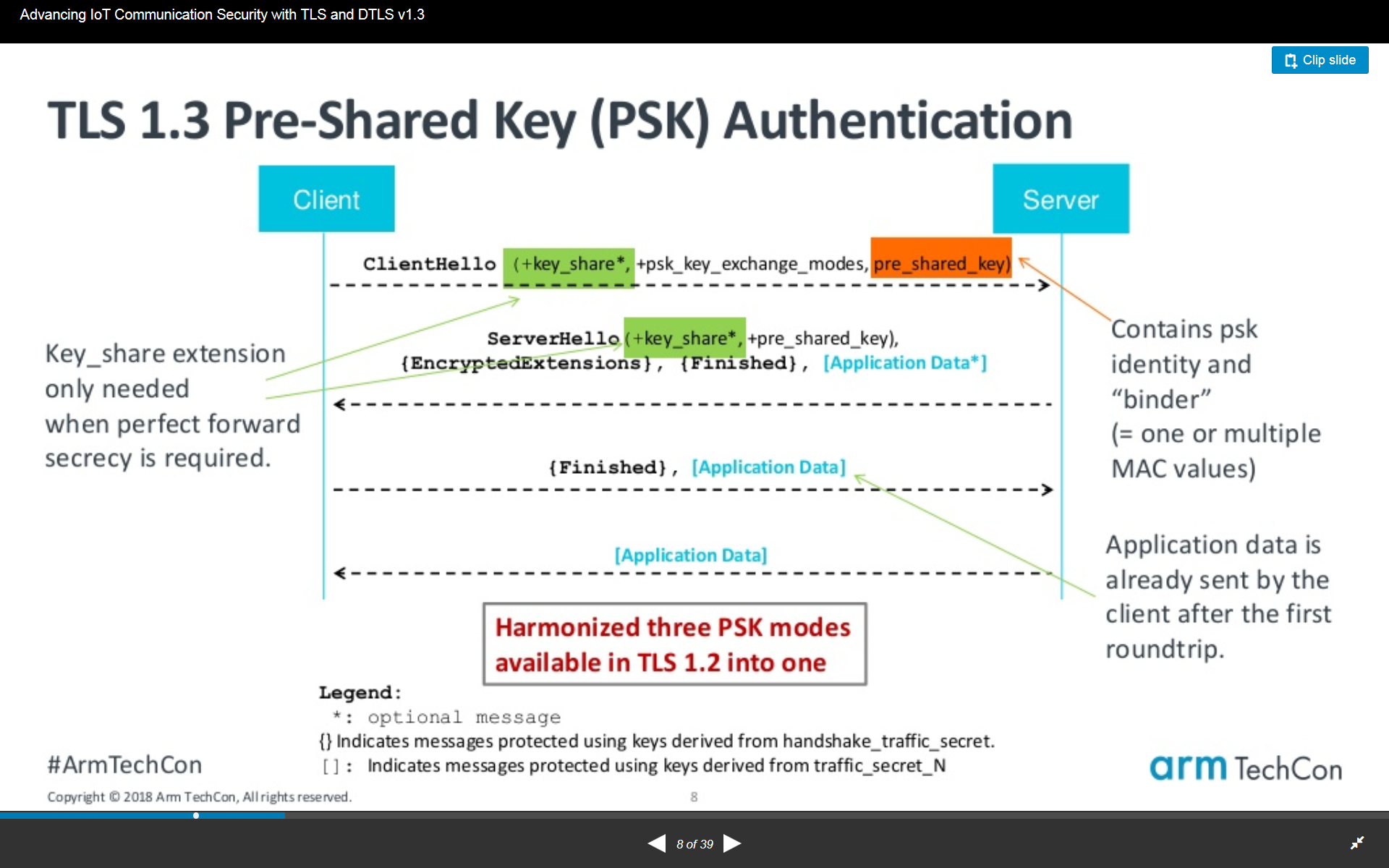


### Symmetric encryption for confidentiality of regular traffic.

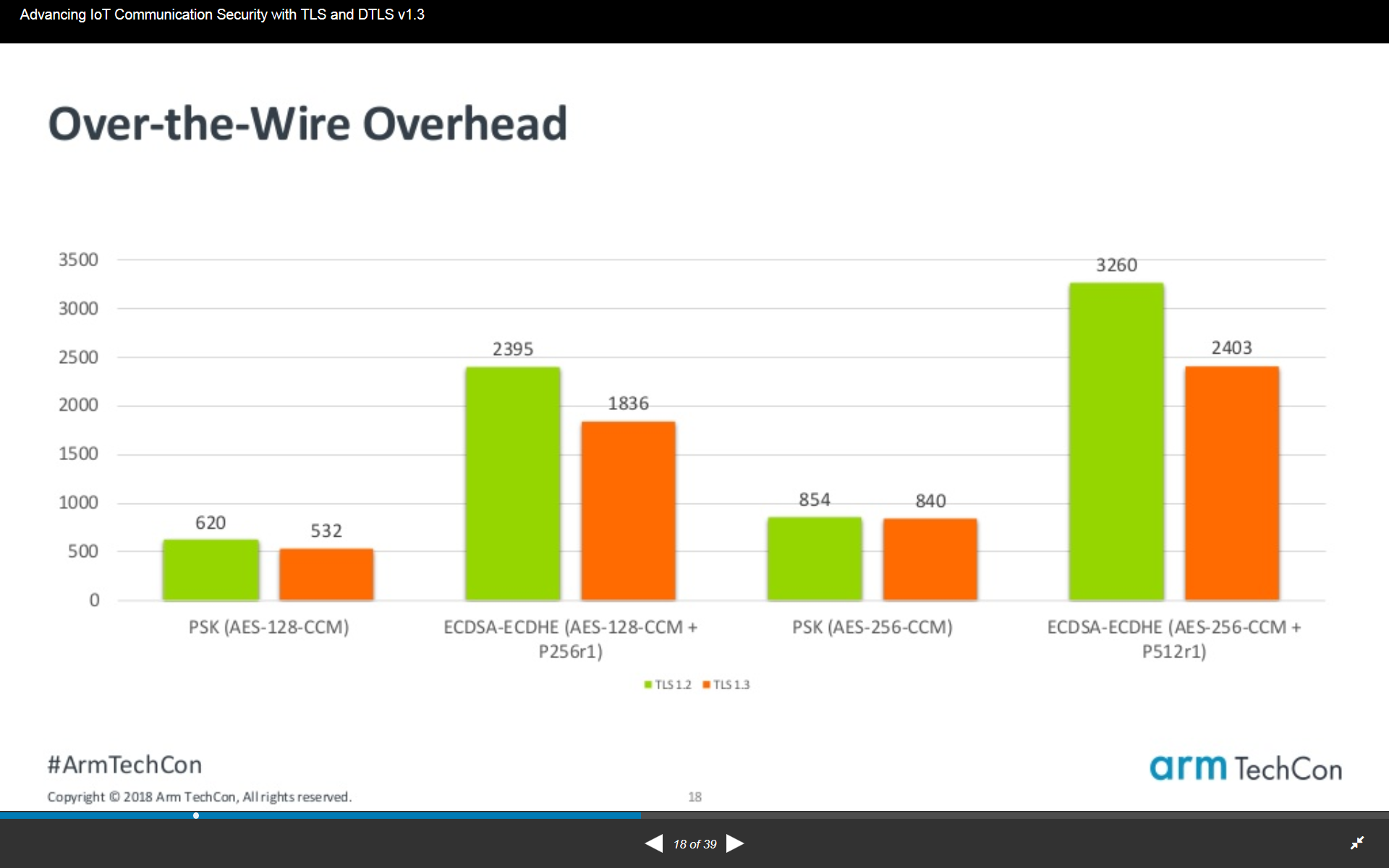
Since devices share key there are two options to encrypt regular traffic (between joined devices or Router):

1. [DTLS PSK ciphersuite](https://en.wikipedia.org/wiki/TLS-PSK) - DTLS based on pre-shared symmetric key
2. or direct use of AES - to minimize traffic between sleepy devices (battery should be alive for long period)

DTLS PSK has less flights (handshakes) than DTLS-JPAKE until client can send application data (compare with J-Pake diagram below):



Below is comparison of overheads between DTLS-PSK (that doesn’t use asymmetric algorithms) and predominantly asymmetric ECDSA-ECDHE(not used here but is close to DTLS-JPAKE):



Code size:



## Authentication and Key Agreement

The Mesh Network is designed to provide a high level of security during the process of adding devices to the network and during normal network operation. During the joining process, devices MUST BE specifically authenticated and authorized, and required to complete a key agreement mechanism. Once on the network, all communications are secured with a network key (DMK). The fundamental security used during the joining for authentication and key agreement is an elliptic curve variant of J-PAKE (EC-JPAKE), using the NIST P-256 elliptic curve. J-PAKE is a PAKE (Password Authenticated Key Exchange) with “juggling” (hence the “J”). It essentially uses elliptic curve Diffie-Hellmann for key agreement and Schnorr signatures as a NIZK (Non-Interactive Zero-Knowledge) proof mechanism to authenticate two peers and to establish a shared secret between them based on the passphrase. Authorization is implied through the entry of the specific passphrase into the commissioning device. A TLS (Transport Layer Security) handshake is used for EC-JPAKE, which can be used in both TLS and DTLS (Datagram Transport Layer Security). DTLS is a variant of TLS with additional fields in the records to make it suitable for use over an unreliable datagram secured with a network key.

### DTLS

Commissioning and joining use the same secure algorithm of secure session: authentication, exchange of encrypted data – DTLS.

MbedTLS is the library that implements DTLS and proposed in this paper.

MbedTLS implements J-PAKE authentication.

Internet of Things (IoT) nodes participating in the implementation of IoT applications will need standard methods to authenticate each other and secure their communications. However, the use of certificates and public key infrastructure (PKI) technologies, widely employed in the Internet, is not straightforward in this context because of the limitations of the involved entities – restricted devices.

### J-PAKE

In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a password-authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a [password](https://en.wikipedia.org/wiki/Password).



An important property is that an eavesdropper or man in the middle cannot obtain enough information to be able to brute force guess a password without further interactions with the parties for each (few) guesses. This means that strong security can be obtained using weak passwords.

**Password authenticated key exchange** (PAKE) is where two or more parties, based only on their knowledge of a password, establish a cryptographic key using an exchange of messages, such that an unauthorized party (one who controls the communication channel but does not possess the password) cannot participate in the method and is constrained as much as possible from brute force guessing the password.

The **Password Authenticated Key Exchange by Juggling** (or J-PAKE) is a [password-authenticated key agreement](https://en.wikipedia.org/wiki/Password-authenticated_key_agreement) protocol

allows two parties to establish private and authenticated communication solely based on their shared (low-entropy) password without requiring a [Public Key Infrastructure](https://en.wikipedia.org/wiki/Public_Key_Infrastructure). It provides [mutual authentication](https://en.wikipedia.org/wiki/Mutual_authentication) to the key exchange, a feature that is lacking in the [Diffie–Hellman key exchange](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange) protocol.

Elliptic curve cryptography is used in J-PAKE implementation in mbedTLS. Also

Schnorr ZKP (Zero Knowledge Proof) is part of J-PAKE.

The two-round J-PAKE protocol is completely symmetric. This helps significantly simplify the security analysis. For example, the proof that one party does not leak any password information in the data exchange must hold true for the other party based on the symmetry. This reduces the number of the needed security proofs by half.

In practice, it is more likely to implement J-PAKE in three flows since one party shall normally take the initiative.

#### Security properties of J-PAKE

Given that the underlying Schnorr non-interactive [zero-knowledge proof](https://en.wikipedia.org/wiki/Zero-knowledge_proof) is secure, the J-PAKE protocol is proved to satisfy the following properties:[[3]](https://en.wikipedia.org/wiki/Password_Authenticated_Key_Exchange_by_Juggling#cite_note-3)

1. Off-line dictionary attack resistance - It does not leak any password verification information to a passive/active attacker.
2. [Forward secrecy](https://en.wikipedia.org/wiki/Forward_secrecy) - It produces session keys that remain secure even when the password is later disclosed.
3. Known-key security - It prevents a disclosed session key from affecting the security of other sessions.
4. On-line dictionary attack resistance - It limits an active attacker to test only one password per protocol execution.

In 2015, Abdalla, Benhamouda and MacKenzie conducted an independent formal analysis of J-PAKE to prove its security in a random oracle model assuming algebraic adversaries.[[4]](http://www.normalesup.org/~fbenhamo/files/publications/SP_AbdBenMac15.pdf)

#### Standardization of J-PAKE

J-PAKE has been included in ISO/IEC 11770-4 (2017) as an international standard.[[11]](https://en.wikipedia.org/wiki/Password_Authenticated_Key_Exchange_by_Juggling#cite_note-11) It is also published in [RFC 8236](https://tools.ietf.org/html/rfc8236)

### Comparison with other authentication systems.

Other well-known auth systems we considered:

* Kerberos (symmetric encryption)
* PKI (asymmetric)

#### Kerberos

[Kerberos for IoT](https://kit.mit.edu/sites/default/files/documents/Kerberos_Internet_of%20Things.pdf): the **Pros**:

- Well understood protocol (cf. Needham-Schroeder);

- Symmetric-key approach suits constrained devices;

– Long-term keys can be installed by device manufacturer;

– Symmetric key operations cheaper/faster;

– Kerberos flows can be optimized for IoT devices;

- Integration with directories a well-trodden path;

- Open source code (20+ years) –MIT code written in C – several generations of coders –Active dev community

Kerberos in IoT: the Cons

- works excellent in corporate environment;

- RFC4120 will put you to sleep...

- No initial key distribution protocol –Use PKINIT (RFC6112) or similar

- Good C programmers hard to come-by

#### PKI

PKI requires expensive infrastructure: signing server, revocation services (CRL or OCSP), sometimes CMP service. There is a big concern with PKI because of the management of the invalidation of certificates.

Some risks:

* System Downtime Due to Certificate Expiries ()
* Management by Spreadsheet

One can only look at the news of IoT devices becoming inoperative, such as the Wink Hub issue in April of 2015, to see that maintaining expiring certificates can cause major problems in the deployment of IoT devices.

PKI for IoT is referred in articles:

1. “[PKIoT: A public key infrastructure for the Internet of Things](https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3681)”
2. [“Technology Insight for X.509 Certificate Management”](https://www.gartner.com/en/documents/3969998/technology-insight-for-x-509-certificate-management)
3. “New research project aims to “shrink” public key infrastructure (PKI) [technology](https://www.nexusgroup.com/public-key-infrastructure-pki-secure-iot/) to secure the IoT”

## MbedTLS implementation of DTLS J-Pake (MBEDTLS\_TLS\_ECJPAKE\_WITH\_AES\_128\_CCM\_8)

mbed TLS is used in embedded software. mbed TLS offers an [SSL library](https://tls.mbed.org/ssl-library) with an intuitive API and readable source code, so you can actually understand what the code does. Also the mbed TLS modules are as loosely coupled as possible and written in the portable C language. This allows you to use the parts you need, without having to include the total library.

mbed TLS is available as open source under the Apache 2.0 license or the GPL 2.0 license. The Apache 2.0 license enables you to use mbed TLS in both open source and closed source projects.

MbedTLS has small memory and storage footprint. To reduce mbed TLS memory and storage footprint:

<https://tls.mbed.org/kb/how-to/reduce-mbedtls-memory-and-storage-footprint>

### Licensing

<https://tls.mbed.org/kb/licensing/using-mbedtls-in-a-non-gpl-project>