THREAD GROUP

July 13, 2015

This Thread Technical white paper is provided for reference purposes only.

The full technical specification is available to Thread Group Members. To join and gain access, please follow this link: http://threadgroup.org/Join.aspx.

If you are already a member, the full specification is available in the Thread Group Portal: http://portal.threadgroup.org.

If there are questions or comments on these technical papers, please send them to help@threadgroup.org.

THREAD GROUP

Thread Commissioning

July 2015

Revision History

Revision	Date	Comments
1.0	January 29, 2015	Initial Release
2.0	July 13, 2015	Public Release

Contents

Introduction

Commissioning is the process whereby a user wants to get the Thread Device they have just bought onto their Thread Network. The aim of this white paper is to show the mechanisms used that ensure a simple user experience based on entering passphrases yet provide a high level of security.

Terminology

Table 0-1. Terms and Definitions

Term	Definition
Border Router	Any device capable of forwarding between a Thread Network and a non-Thread Network. The Border Router also serves as an interface point for the Commissioner when the Commissioner is on a non-Thread Network. The Border Router requires a Thread interface to perform and may be combined in any device with other Thread roles except the Joiner.
Commissioner	The currently elected authentication server for new Thread 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 Thread interfaces may perform this role, but those that have them may combine this role with all other roles except the Joiner. 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 Leader 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

Term	Definition
	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 initial Leader, 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.
Joiner	The device to be added by a human administrator to a commissioned Thread Network. This role requires a Thread interface to perform and cannot be combined with another role in one device. The Joiner does not have network credentials.
Joiner Router	An existing Thread router or REED (Router-Eligible End Device) on the secure Thread Network that is one radio hop away from the Joiner. The Joiner Router requires a Thread interface to operate, and may be combined in any device with other roles except the Joiner role.
Joining	The process of authenticating and authorizing a Thread Device onto the Thread Network.
Joining Passphrase	An 8-to 16-digit alphanumeric string using a limited set of characters for authenticating a Joiner. The passphrase is deliberately lower strength than the key that will be produced using the associated PAKE.
J-PAKE	PAKE with juggling
KEK	Key Establishment Key used to secure delivery of the network-wide key and other network parameters to the Joiner.
Leader	The device responsible for managing router ID assignment.

Term	Definition
	The single distinguished device in any Thread Network that currently acts as a central arbiter of network configuration state. The Leader requires a Thread interface to perform and may be combined in any device with other roles except the Joiner.
PAKE	Password authenticated key exchange
Petitioning	The process of authenticating and authorizing a Commissioner Candidate onto the Thread Network through a representative (typically the Border Router).
Thread Device	A device that participates directly in the Thread Network.
Thread Network	The 802.15.4 and 6LoWPAN-based mesh network allowing communication between Thread Devices.
TMF	Thread Management Framework
User	The home/premises owner who controls the Thread Network and the home/premises WLAN.
WLAN	The wireless LAN (Local Area Network) in the home/premises, typically Wi-Fi. Other LAN technologies could be considered (for example,, powerline) as well but are assumed to function in a similar manner to a WLAN.

System Topology

Commissioning must be able to take place in a system where a Joiner that wishes to participate in the Thread Network is authenticated using a device known as a Commissioner. In the broadest sense, the Commissioner should only need to find some level of online connectivity to the Thread Network; this could be through the Internet or a cloud service. However, initially it will be assumed that the Commissioner will have online connectivity to the Thread Network locally in the premises through the WLAN or directly participating in the Thread Network. When connectivity is provided through the WLAN, the Commissioner is known as an external Commissioner. When connectivity is provided through the Thread Network, the Commissioner is known as a Native Commissioner.

Degrees of Separation

From a topology point of view, there are four cases which will be considered:

External Commissioner is connected to the WLAN

1. Border Router is not Joiner Router (Figure 1)
2. Border Router is Joiner Router (Figure 2)

Native Commissioner is connected to the Thread Network

3. Joiner Router is not Commissioner (Figure 3)
4. Joiner Router is Commissioner (Figure 4)

This means the Commissioner will be:

- In direct communication with the Joiner (case 4)
- One degree of separation from the Joiner (cases 2 and 3)
- Two degrees of separation from the Joiner (case 1)

In the cases where there are one or more degrees of separation, relay agents and relay client/server bindings are deployed to relay the DTLS (Datagram Transport Layer Security) handshake between Joiner and Commissioner using the Commissioning Relay and TMF (Thread Management Framework) Relay protocol. The relay agents will exist on the Joiner Router and the Border Router and ideally retain no state about the Joiner.

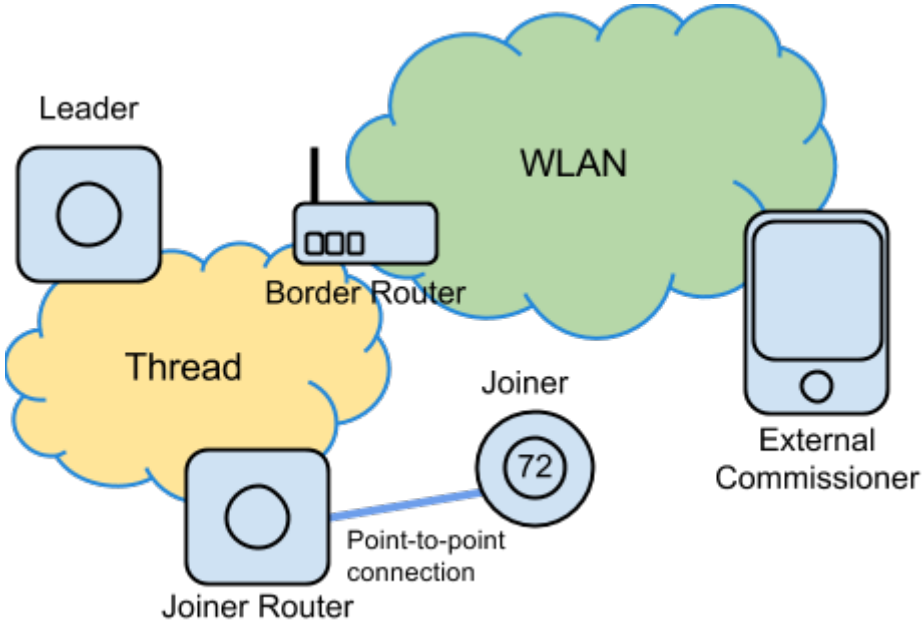

Figure 1. Case 1: External Commissioner connected to the WLAN, Border Router is not Joiner Router

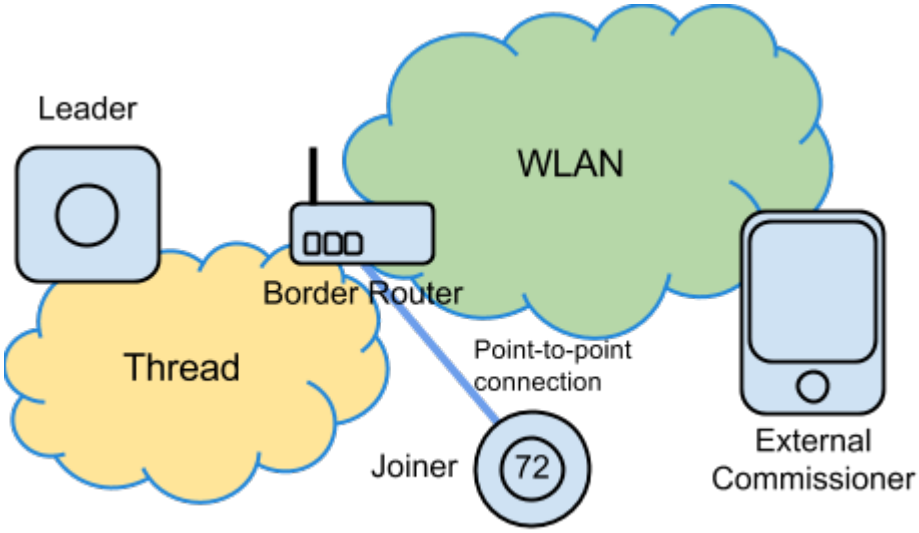

Figure 2. Case 2: External Commissioner connected to the WLAN, Border Router is Joiner Router

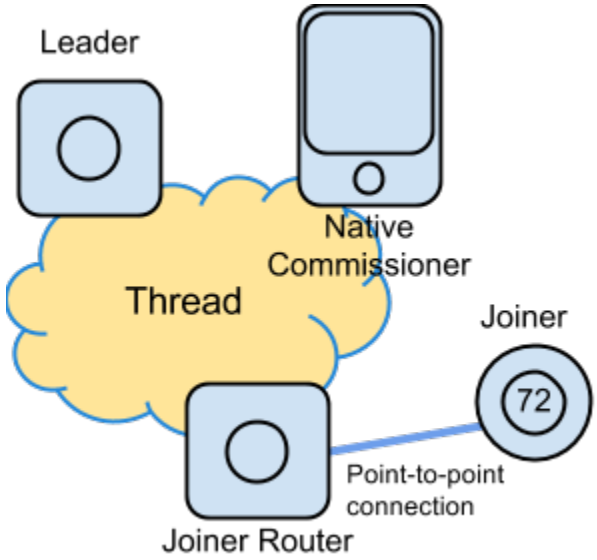

Figure 3. Case 3: Native Commissioner connected to the Thread Network, Joiner Router is not Commissioner

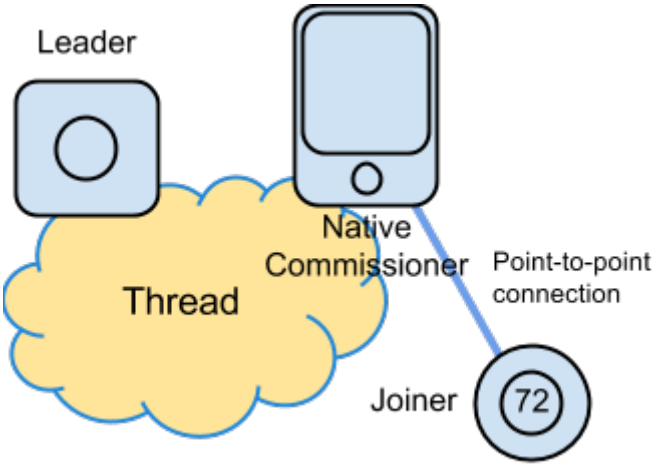

Figure 4. Case 4: Native Commissioner connected to Thread Network, Joiner Router is Commissioner

Security Fundamentals

Authentication and Key Agreement

The fundamental security used in the Thread Network is an elliptic curve variant of J-PAKE (EC-JPAKE), using the NIST P-256 elliptic curve. J-PAKE is a password-authenticated key exchange (PAKE) 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. The author has published two internet drafts which describe J-PAKE [draft-hao-jpake-01] and the Schnorr NIZK proof [draft-hao-schnorr-01].

A TLS (Transport Layer Security) 1.2 [RFC 5246] handshake will be developed for EC-JPAKE, which can potentially be used in both TLS and DTLS. DTLS [RFC 6347] is a variant of TLS with additional fields in the records to make it suitable for use over an unreliable datagram-based transport (for example,, UDP (User Datagram Protocol), whereas TLS assumes a reliable transport such as TCP (Transport Control Protocol).

Network-wide Key

The Thread Network is protected with a network-wide key, which is used at the MAC (Media Access Control) layer 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 Thread Network from outsiders without knowledge of the network-wide key. As it is a network-wide key, compromise of any Thread Device could potentially reveal the key; therefore, it is not typically used as the only form of protection within the Thread Network. From the point of view of joining, it is used to discriminate between an authenticated and authorized Thread Device and the Joiner (in its initial state). The network-wide key, along with other network parameters, is delivered securely to a Joiner using a KEK (Key Encryption Key) to secure it.

Authentication

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

In the case where the Commissioner is not in direct communication with the Joiner, the Joiner Router must relay the DTLS handshake with the Commissioner. The Commissioning relay protocol provides encapsulation of the DTLS handshake and relaying of the DTLS handshake from the Joiner all the way to the Commissioner in a simple manner.

Maintenance

The Commissioner uses the Commissioning protocol to keep a secure Communication session alive and also to change certain parameters of the network, for example, the network name.

Commissioning Process

The commissioning process has two phases:

- Petitioning
- Joining

Petitioning must occur before any Joiner can join, that is, there must be one sole authorized Commissioner–the authenticator for subsequent Joiners.

Commissioning Protocol

The MeshCoP (mesh commissioning protocol) is based on CoAP [RFC 7252] and performs petitioning, maintenance, management and relay functions. It is either used in the WLAN or in the Thread Network and is based on the TMF.

Petitioning

External Commissioner Candidate

If the Commissioner Candidate uses a WLAN network interface for commissioning purposes, it is known as an external Commissioner. An external Commissioner has to petition the Thread Network through a representative (the Border Router) to become the sole authorized Commissioner. The Commissioner Candidate must use an authentication handshake with the Border Router to prove it is eligible to become the sole authorized Commissioner and set up a secure Commissioning session. The Commissioner Candidate then petitions the Leader via the Border Router because there can be only one authorized Commissioner. If petitioning succeeds, the Commissioner Candidate becomes the sole authorized external Commissioner. The secure Commissioning Session remains in place, the representative Border Router will be made known throughout the Thread Network and all subsequent communication with other Thread devices

will be done through the Border Router. A periodic keep-alive message is sent on the secure Commissioning session to ensure it remains open.

Figure 5 illustrates the External Commissioner petitioning.

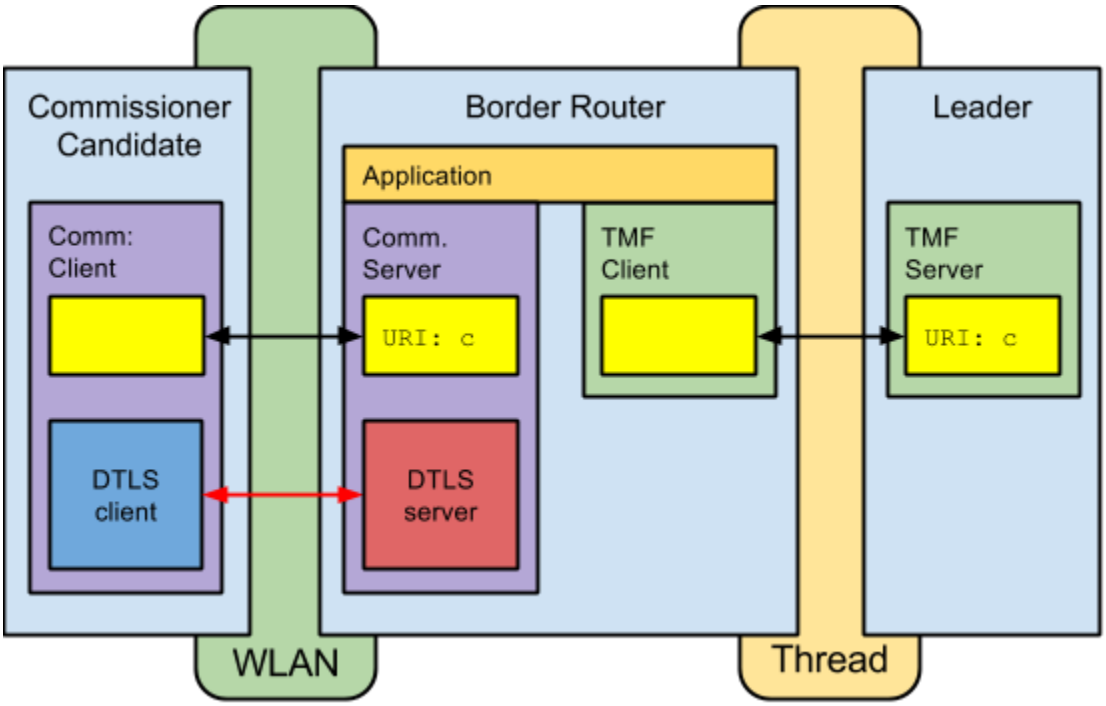

Figure 5. External Commissioner Petitioning

1. The process starts with the Border Router being aware of the Commissioner Credential. This can be entered directly into the Border Router device itself or into any trusted Thread Device and sent to the Border Router.
2. Sometime later, the same Commissioner Credential will be entered into the Commissioner Candidate and the Commissioner Candidate will initiate the registration process, starting with a DTLS handshake. If the DTLS handshake is successful, the Border Router will have authenticated the Commissioner Candidate based on knowledge of the shared Commissioner Credential.
3. The Border Router will arbitrate with the Leader on behalf of the Commissioner Candidate to authorize the Commissioner Candidate to be the sole Commissioner and authenticator for subsequent Joiners. If there is already an authorized Commissioner, the Commissioner Candidate will be denied authorization.

4. The authorized Commissioner will keep a secure Commissioning session open with the Border Router, which can use the DTLS record layer for encryption and authentication based on keys derived from the master key established between the Commissioner (as the Commissioner Candidate) and the Border Router as a result of the DTLS handshake. This session Commissioning session will be used for various purposes and will communicate CoAP messages carrying petitioning, management and relay messages between the Commissioner and the Border Router.

Figure 6 illustrates the External Commissioner petitioning sequence.

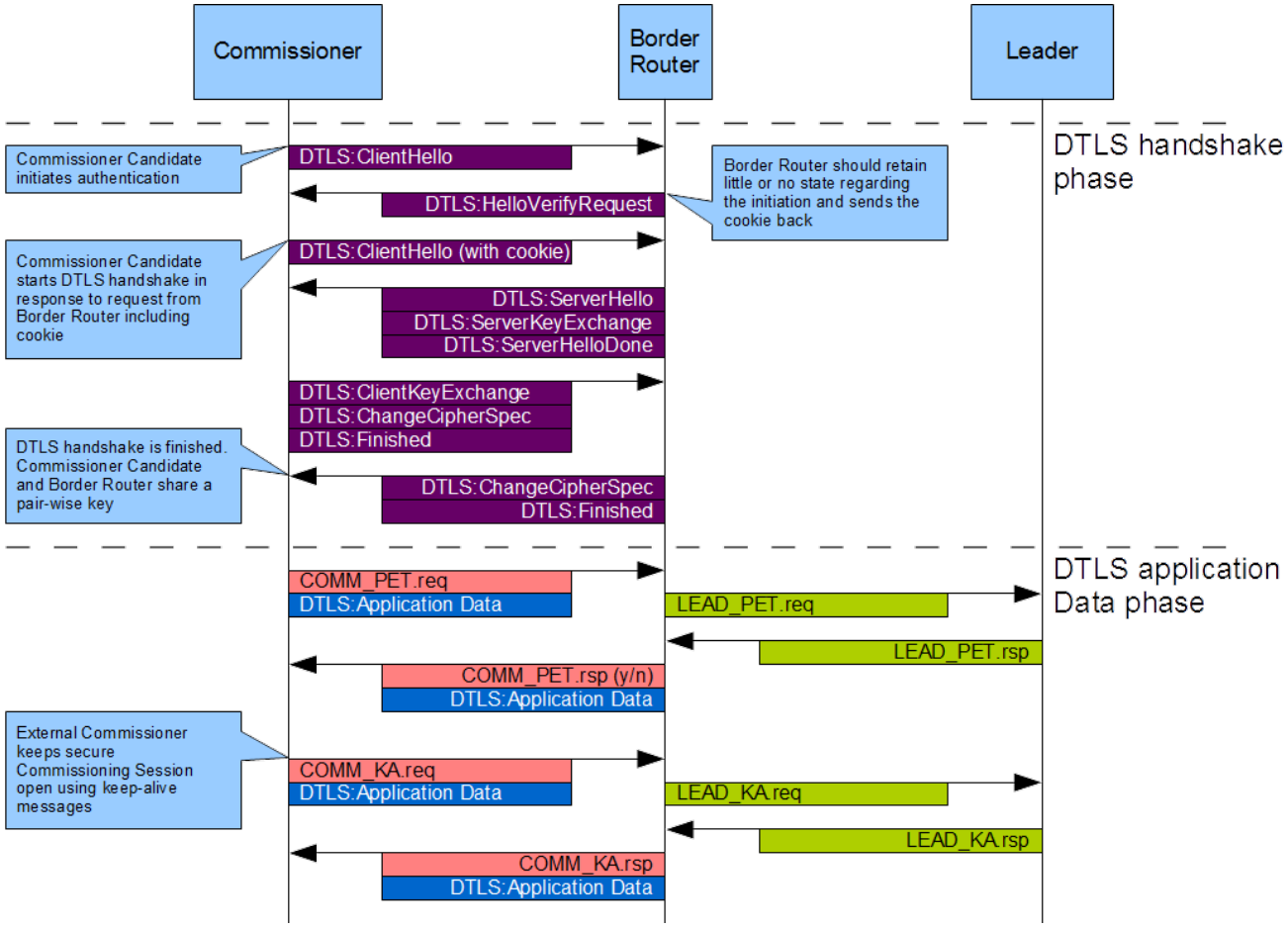

Figure 6. External Commissioner Petitioning Sequence

Native Commissioner Candidate

If the Commissioner Candidate uses a Thread Network interface for commissioning purposes, it is known as a Native Commissioner. A Native Commissioner has to petition the Thread Network through a representative (the Commissioner Router) to become the sole authorized Commissioner. The Commissioner Candidate must use an authentication handshake with the Commissioner Router to prove it is eligible to become the sole authorized Commissioner and set up a secure Commissioning session. The Commissioner Candidate then petitions the Leader via the Commissioner Router because there can be only one authorized Commissioner. If petitioning succeeds, the Commissioner Candidate becomes the sole authorized Native Commissioner. However, the Commissioner subsequently joins the Thread Network and becomes an active device (on-mesh Commissioner) and all communication with other Thread devices takes place directly with the Commissioner.

Figure 7 illustrates the Native Commissioner petitioning.

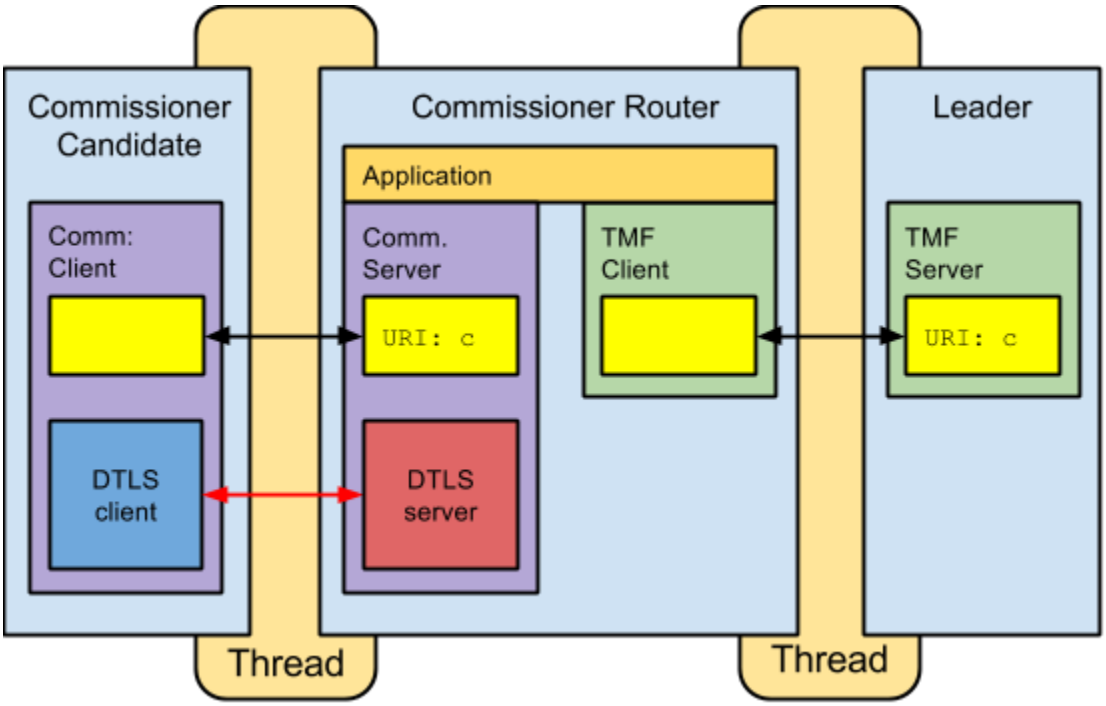

Figure 7. Native Commissioner Petitioning

1. The process starts with the Commissioner Router being aware of the Commissioner Credential. This can be entered directly into the Commissioner Router device itself or into any trusted Thread Device and sent to the Commissioner Router.
2. Sometime later, the same Commissioner Credential will be entered into the Commissioner Candidate and the Commissioner Candidate will initiate the registration process, starting with a DTLS handshake. If the DTLS handshake is successful, the Commissioner Router will have authenticated the Commissioner Candidate based on knowledge of the shared Commissioner Credential.
3. The Commissioner Router will arbitrate with the Leader on behalf of the Commissioner Candidate to authorize the Commissioner Candidate to be the sole Commissioner and authenticator for subsequent Joiners. If there is already an authorized Commissioner, the Commissioner Candidate will be denied authorization.
4. The authorized Commissioner will subsequently join the Thread Network and thus be able to communicate directly with all Thread Devices.

Figure 8 illustrates the Native Commissioner petitioning sequence.

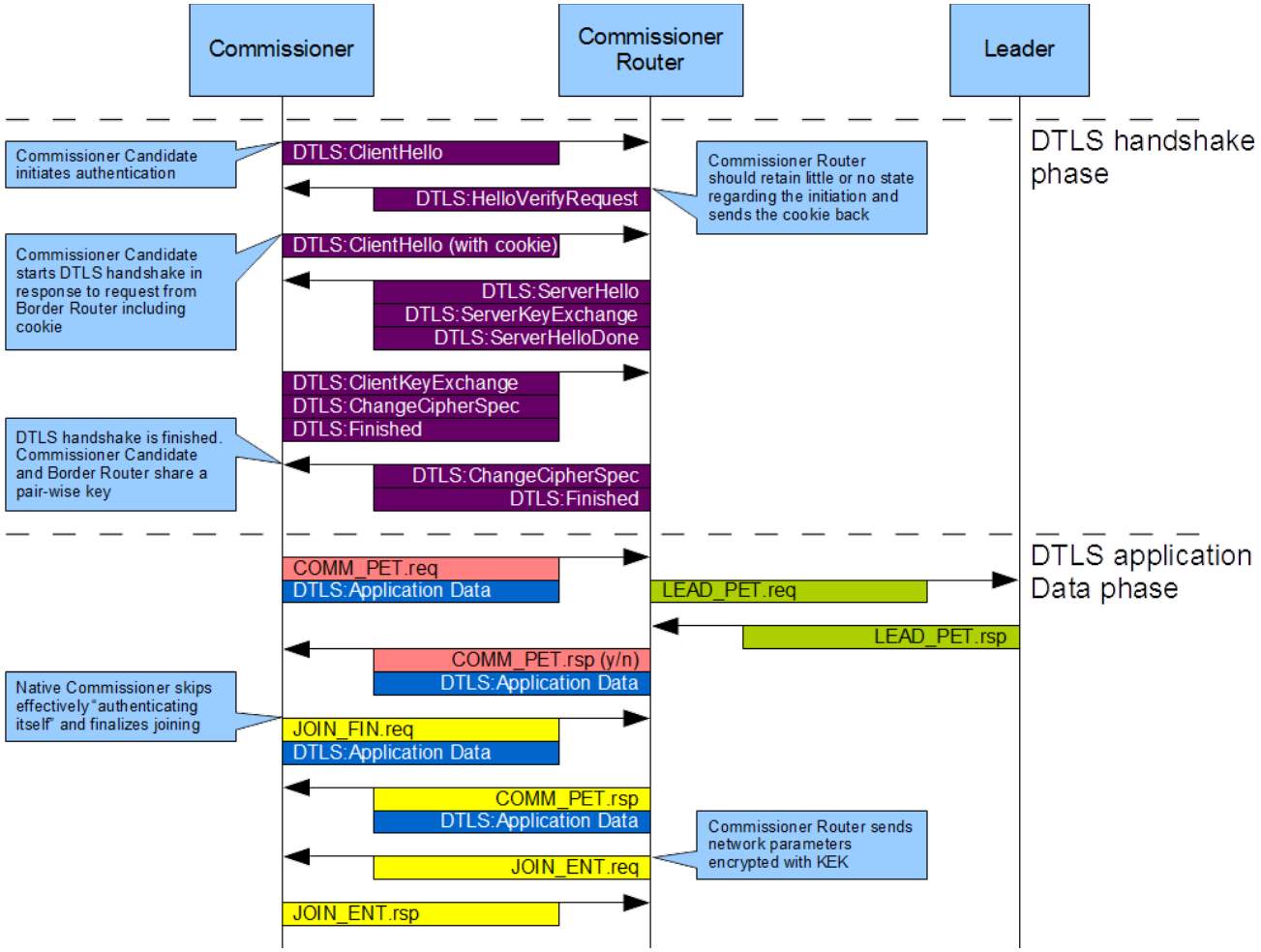

Figure 8. Native Commissioner Petitioning Sequence

Petitioning Authorization

When a Border Router or Commissioner Router receives a petitioning request from the Commissioner Candidate, the Border Router/Commissioner Router relays the petitioning request to the Leader with the ID of the Commissioner Candidate. The Leader will respond by accepting or rejecting the request and the Border Router will relay the response accordingly. If the Commissioner Candidate is external, the Leader will also advertise the Border Router acting on behalf of the Commissioner to the rest of the Thread Network so any potential Joiner Router knows where to relay DTLS handshake messages originating from the Joiner. In addition, the

beacon information will be updated through a notification so all Thread Routers alter their beacon, assisting steering of the Joiner.

Figure 9 illustrates the petitioning authorization.

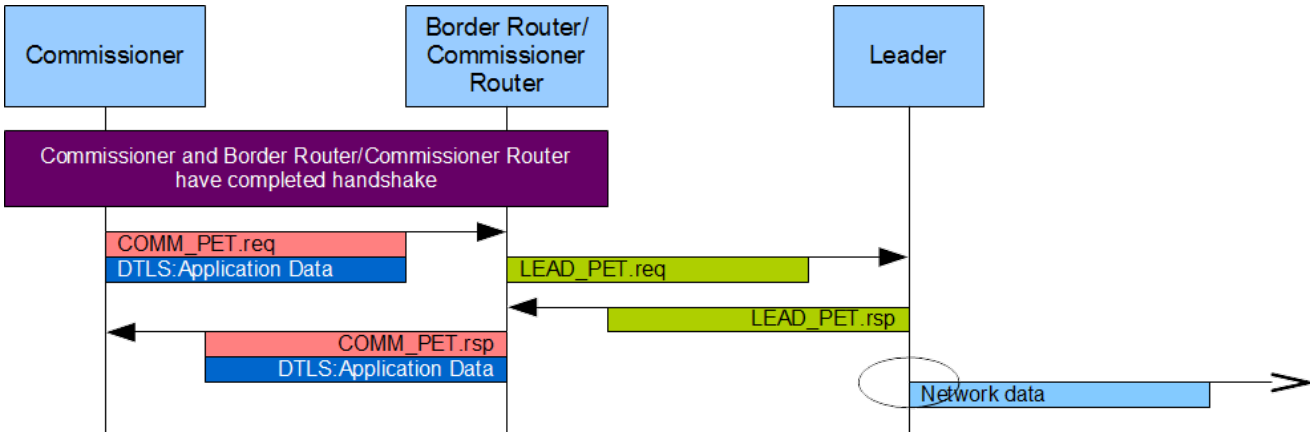

Figure 9. Petitioning Authorization

Joining

When there is an authorized Commissioner associated with the Thread Network, it becomes possible to join eligible Thread Devices. These are known as Joiners before they can actively participate in the Thread Network. The actual joining process depends on the system topology as described in System Topology. As a reminder, there are four clearly identifiable scenarios:

External Commissioner is connected to the WLAN

1. Border Router is not Joiner Router
2. Border Router is Joiner Router

Native Commissioner is connected to the Thread Network

3. Joiner Router is not Commissioner
4. Joiner Router is Commissioner

External Commissioner Is Connected to the WLAN

In this case, the Petitioning process as described in **External Commissioner Candidate** must have taken place initially to provide a secure Commissioning session from Border Router to Commissioner bound to the petitioning process. This secure session is then used in the Joining process to relay the joining DTLS handshake through to the Commissioner. Once the Joiner has

received the network parameters it needs to attach to the Thread Network, it closes the secure Commissioning session.

Border Router Is Not Joiner Router

This is the most complex case to consider in the four presented scenarios. In this case, there are three separate and distinct paths the authentication traffic (the DTLS handshakes) has to go through:

- Joiner to Joiner Router point-to-point
- Joiner Router to Border Router through Thread Network
- Border Router to Commissioner through WLAN

These paths are effectively connected to each other and the Joiner Router and Border Router's relay agents and client/server bindings marshal authentication traffic accordingly (Figure 10).

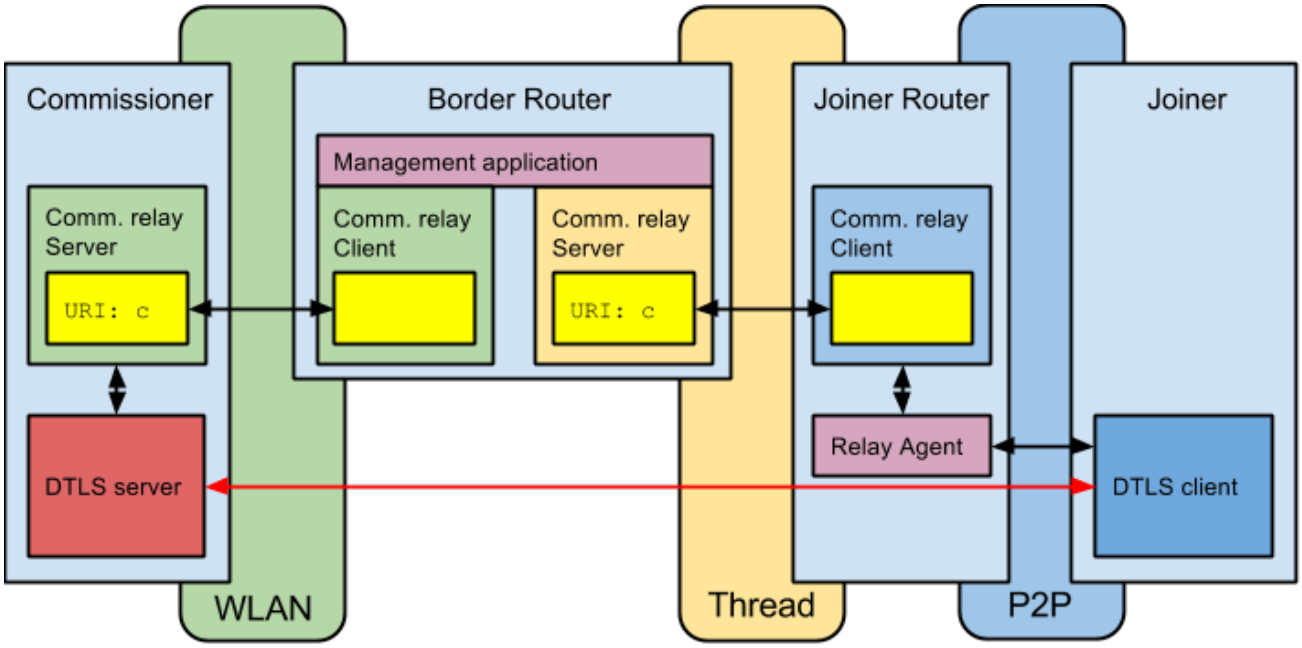

Figure 10. Joiner–Joiner Router–Border Router–Commissioner

Joiner to Joiner Router Point-to-Point

This communication is over an unsecured, one-hop 802.15.4 radio link and all traffic between the Joiner and Joiner Router will be sent in the clear without any form of integrity checking. This fundamentally means the Joiner Router has to treat any traffic from the Joiner as completely

unauthenticated. Normally, the Thread Network would be in a "lock down" mode, which would cause any Thread Device on the perimeter to ignore any unsecured 802.15.4 traffic. However, when joining is permitted, Joiner Routers should carefully police unsecured 802.15.4 traffic and assume it to be authentication traffic.

The DTLS handshake will occur as initial communication being established between the Joiner and Joiner Router. This uses UDP on a specific port, which allows it to be distinguished from other traffic. A relay agent will police the incoming traffic and the Joiner Router will relay the DTLS client handshake along with address and port details of the Joiner and the Joiner Router itself to the Border Router. The address and port details ensure relayed DTLS server handshake response messages can be relayed back through the Joiner Router to the originating Joiner.

Joiner Router to Border Router through Thread Network

This communication is over the Thread Network, which will be secured hop-by-hop at the 802.15.4 link layer. It is assumed that there is connectivity over one or more hops between the Joiner Router and the Border Router. The Joiner Router will relay authentication traffic to and from the Border Router using relay messages carrying the DTLS handshake packets along with address and port details.

Border Router to Commissioner through WLAN

This communication over the WLAN uses the existing secure Commissioning session set up between the Border Router and the Commissioner, maintained by Commissioning keep-alive notifications. The Commissioning Relay receive and transmit messages are used to carry the DTLS Handshake to and from the Commissioner and the messages are secured at the DTLS record layer based on the secure Commissioning session.

Figure 11 illustrates the Joiner–Joiner Router–Border Router–Commissioner sequence.

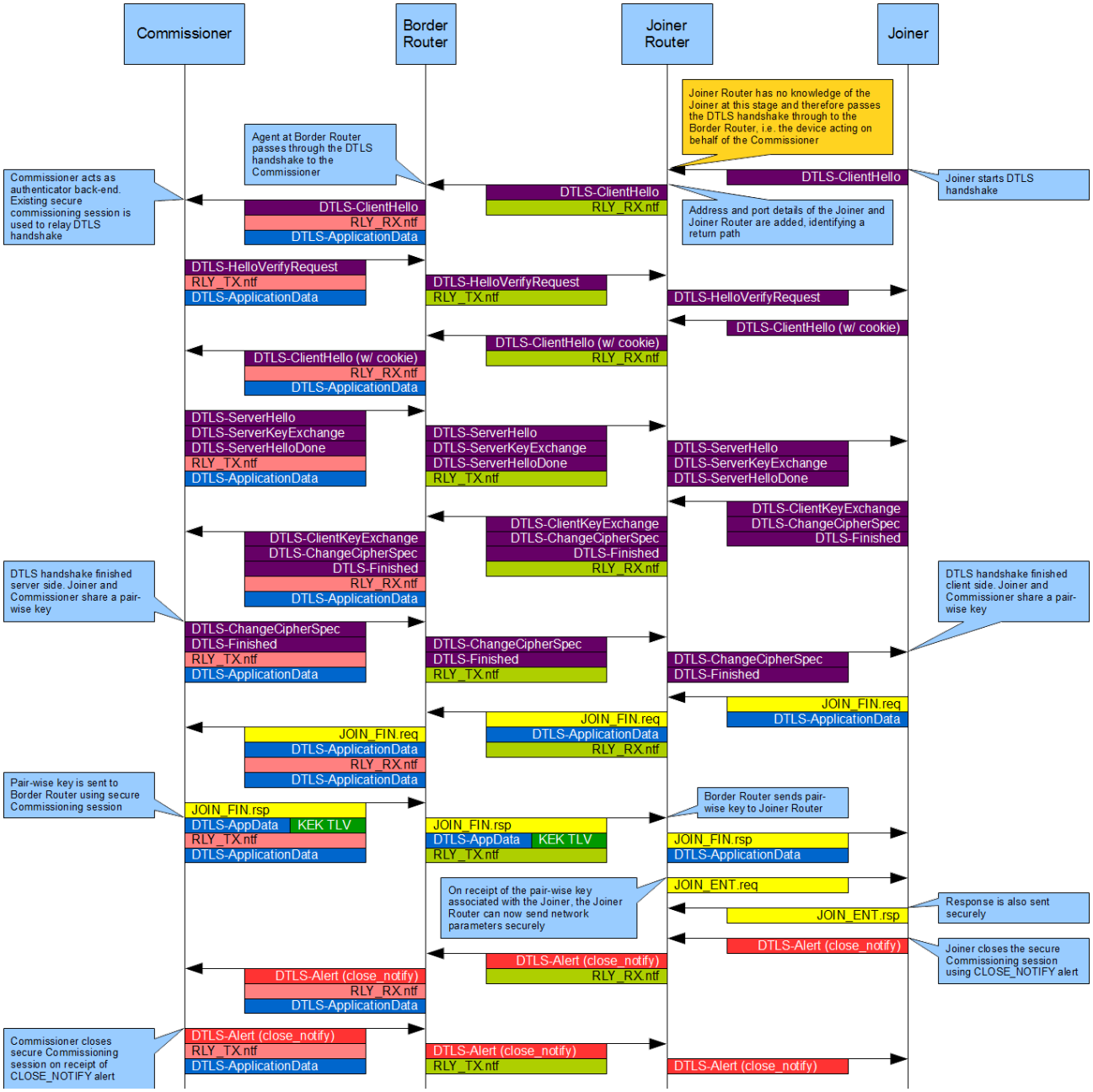

Figure 11. Joiner–Joiner Router–Border Router–Commissioner Sequence

Border Router is Joiner Router

This case is simpler because there is no need to relay from a Joiner Router to a Border Router. However, in this case, the Border Router uses its relay agent to police unauthenticated traffic as a Joiner Router. In this case, there are two separate and distinct paths the authentication traffic (the DTLS handshakes) have to go through:

- Joiner to Border Router point-to-point (as described in **Joiner to Joiner Router Point-to-Point**)
- Border Router to Commissioner through WLAN (as described in **Border Router to Commissioner through WLAN**)

Figure 12 illustrates the Joiner–Joiner Router/Border Router–Commissioner and Figure 13 illustrates the Joiner–Joiner Router/Border Router–Commissioner sequence.

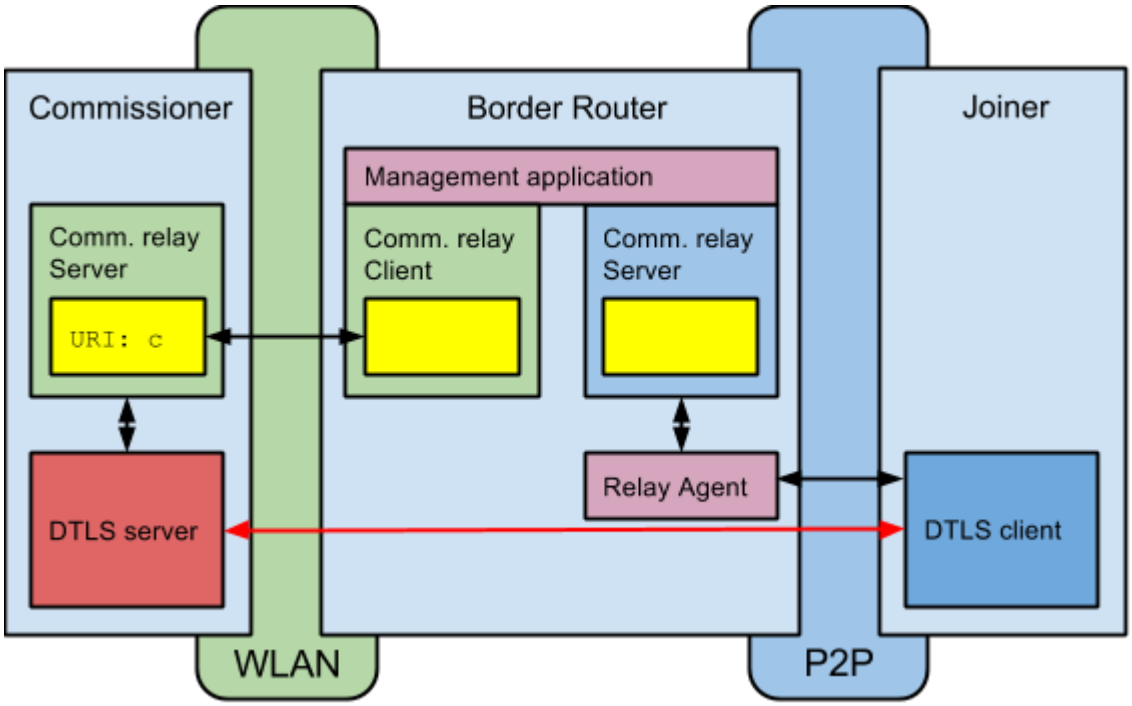

Figure 12. Joiner–Joiner Router/Border Router–Commissioner

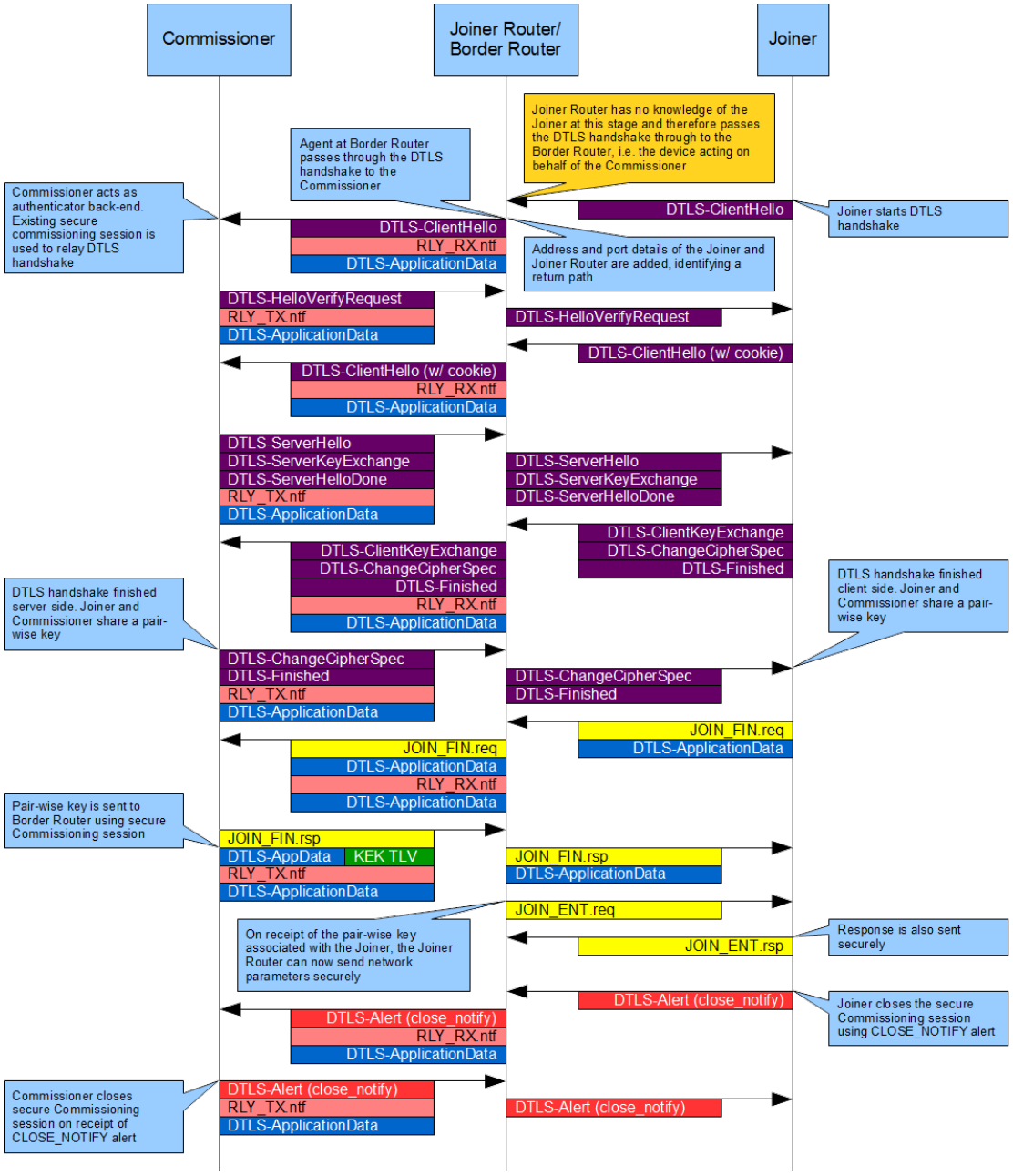

Figure 13. Joiner–Joiner Router/Border Router–Commissioner sequence

Native Commissioner Is Connected to the Thread Network

In this case, either the Petitioning process as described in **Native Commissioner Candidate** must have taken place initially, or the Commissioner has already joined the Thread Network, either by starting it or by using an out-of-band process. Once the Joiner has received the network parameters it needs to attach to the Thread Network, it closes the secure Commissioning session.

Joiner Router Is Not Commissioner

This case is simpler as there is no need to relay from the Border Router to the Commissioner. In this case, there are two separate and distinct paths the authentication traffic (the DTLS handshakes) has to go through:

- Joiner to Joiner Router point-to-point (as described in **Joiner to Joiner Router Point-to-Point**)
- Joiner Router to Commissioner through Thread Network (as described in **Joiner Router to Border Router through Thread Network**, noting in this case the Border Router is the Commissioner)

Figure 14 illustrates the Joiner–Joiner Router–Commissioner and Figure 15 illustrates the Joiner–Joiner Router–Commissioner sequence.

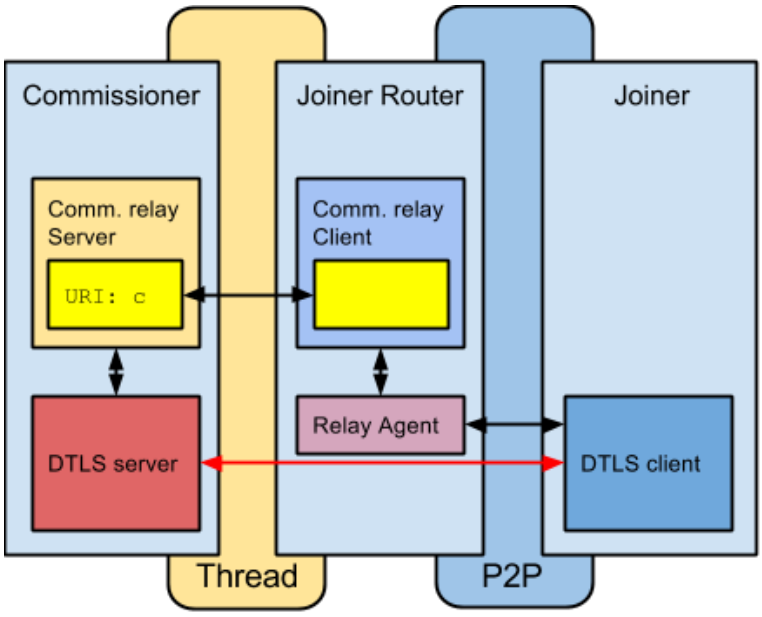

Figure 14. Joiner–Joiner Router–Commissioner

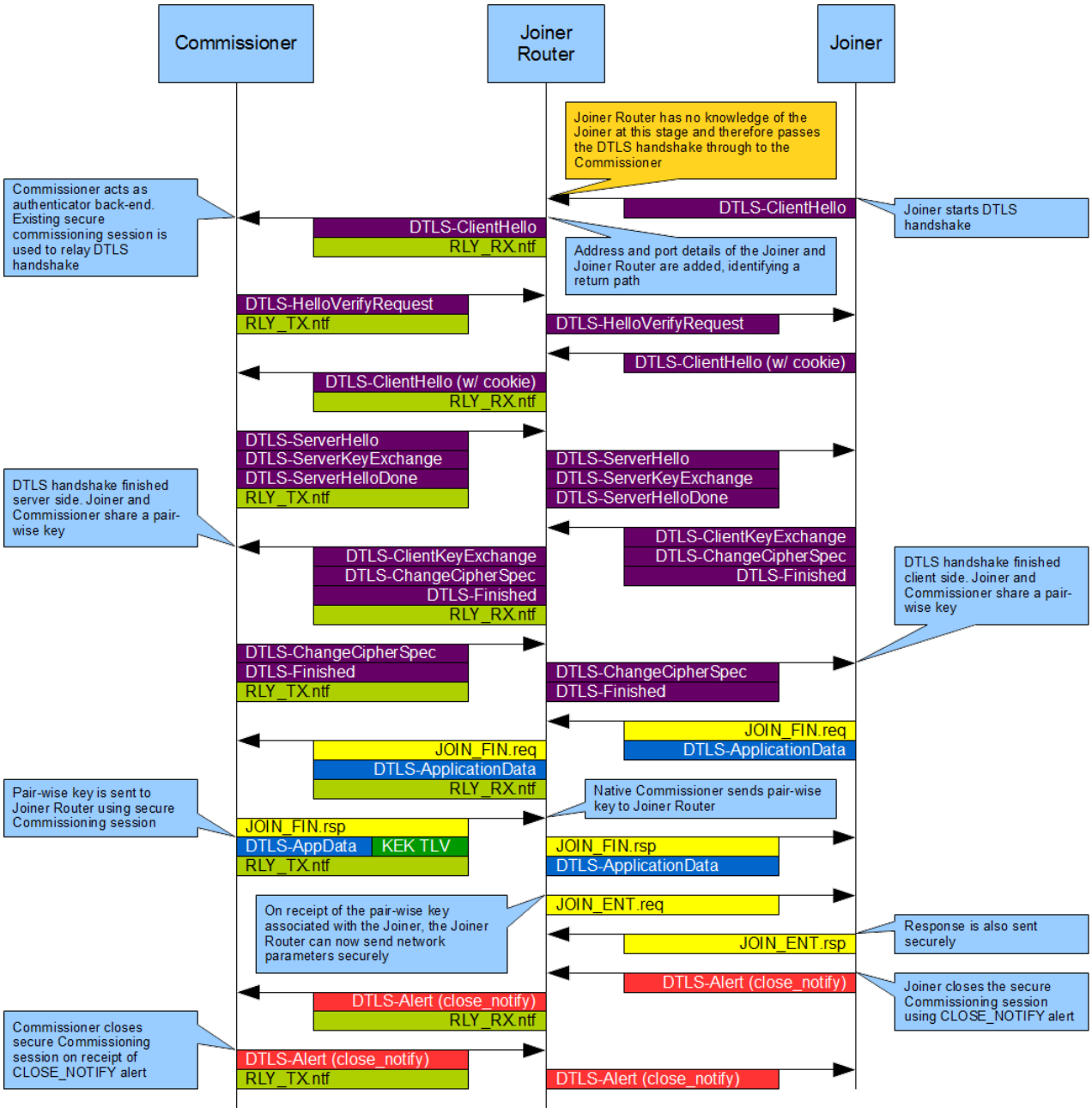

Figure 15. Joiner–Joiner Router–Commissioner Sequence

Joiner Router Is Commissioner

This case is the simplest because there is no need to relay from the Border Router to the Commissioner nor is there a distinct Joiner Router. In this case, there is only one distinct path the DTLS handshake has to go through:

- Joiner to Border Router point-to-point (as described in **Joiner to Joiner Router Point-to-Point**)

Figure 16 illustrates the Joiner–Joiner Router/Commissioner and Figure 17 illustrates the Joiner–Joiner Router/Commissioner sequence.

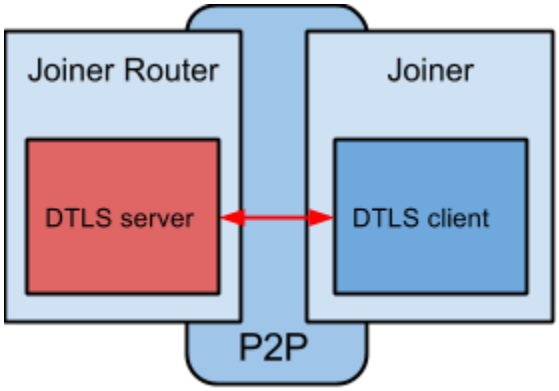

Figure 16. Joiner–Joiner Router/Commissioner

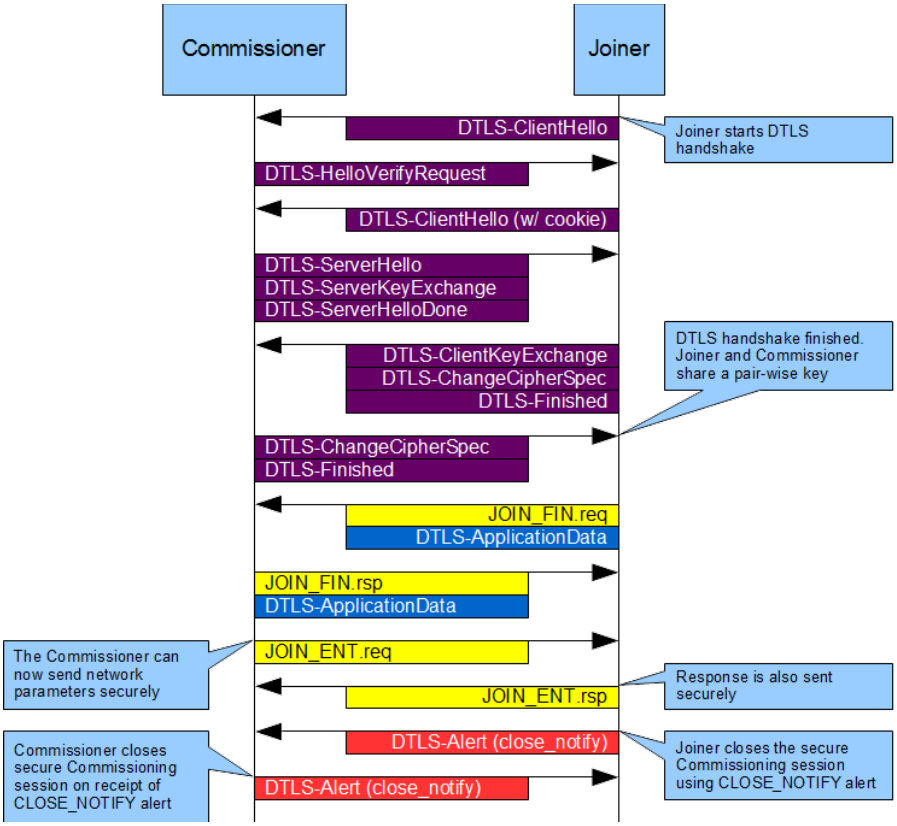

Figure 17. Joiner–Joiner Router/Commissioner Sequence

References

Document	Title
draft-hao-jpake-01	J-PAKE: Password Authenticated Key Exchange by Juggling
draft-hao-schnorr-01	Schnorr NIZK Proof: Non-interactive Zero Knowledge Proof for Discrete Logarithm
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 6347	Datagram Transport Layer Security Version 1.2
RFC 7252	The Constrained Application Protocol (CoAP)