International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.9978

Amendment 1

(05/2022)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Access networks – In premises networks

Secure admission in a G.hn network

Amendment 1

Recommendation ITU-T G.9978 (2018) – Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999
Metallic access networks	G.9700–G.9799
Optical line systems for local and access networks	G.9800–G.9899
In premises networks	**G.9900–G.9999**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.9978

Secure admission in a G.hn network

Amendment 1

Summary

Recommendation ITU-T G.9978 specifies the various secure admission methods for a node to enter a G.hn domain, including media access control (MAC) authorization-based secure admission, generic pairing, auto-pairing and passphrase-based secure admission. This latest revision includes new use cases.

Amendment 1 adds support for native authentication and external authentication, as specified in Recommendation ITU-T G.9961.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.9978	2018-02-09	15	11.1002/1000/13341
2.0	ITU-T G.9978	2018-11-29	15	11.1002/1000/13779
2.1	ITU-T G.9978 (2018) Amd. 1	2022-05-22	15	11.1002/1000/14911

Keywords

G.hn, pairing, push button, secure admission, security.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T G.9978

Secure admission in a G.hn network

Amendment 1

Editorial note: This is a complete-text publication. Modifications introduced by this amendment are shown in revision marks relative to Recommendation ITU-T G.9978 (11/2018).

1 Scope

This Recommendation specifies secure admission methods that are needed for a G.hn node to establish a secure domain (SD) and admit other G.hn nodes to the SD. These methods include media access control (MAC) authorization-based Nsecure admission, push button pairing, auto-pairing and passphrase-based secure admission. The Recommendation also specifies the mechanism for selecting appropriate secure admission methods and addresses interactions between these different secure admission methods.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.9961] Recommendation ITU-T G.9961 (~~2015~~2018), *Unified high-speed wireline-based home networking transceivers – Data link layer specification*.

[ISO/IEC 8859-1] International Standard ISO/IEC 8859-1:1998, *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 auto-pairing: A pairing operation that starts automatically when an unconnected node is powered on.

3.2.2 default non-secure domain name: The domain name specified as the default to be used in a non-secure domain.

3.2.3 generic pairing: Any pairing operation different from auto-pairing. Generic pairing can be started with push buttons or any other mechanism (console command, messages, web interface, etc.) that generates push events.

3.2.4 joining node: A non-secure node that is in the process of either creating a secure domain or entering an already existing secure domain.

3.2.5 MAC authorization-based secure admission: Authentication method for admitting nodes in a secure domain that is based on the comparison of the registration identifier [REGID; media access control (MAC) address] of the registering node with a list of authorized MAC addresses.

3.2.6 multi-node pairing: Pairing procedure that allows several non-secure nodes to join a secure domain during a single pairing window.

3.2.7 non-secure domain (NSD): Domain where communication between nodes is not encrypted.

3.2.8 non-secure domain name: The domain name used in a non-secure domain.

3.2.9 non-secure node: A node that has not been authenticated. It can be connected to other nodes, with non-encrypted traffic, or not connected to any node, i.e., unconnected.

3.2.10 non-secure active node: A non-secure node that can communicate with other nodes using non-encrypted traffic.

3.2.11 pairing window: The time during which non-secure nodes can be authenticated in order to be admitted to a secure domain during an auto-pairing or generic pairing procedure.

3.2.12 pairing window duration: The length of time that the pairing window remains open.

3.2.13 passphrase: Human-readable pattern that is used by some standard admission methods to generate the G.hn password.

3.2.14 password (PW): A standard 96-bit parameter that is used in the G.hn authentication procedure.

3.2.15 PUSH event: Event used to trigger a pairing or unpairing operation.

NOTE – See PUSH-P event and PUSH-R event.

3.2.16 PUSH-P event: Event used to trigger the start of a pairing operation.

3.2.17 PUSH-R event: Event used to trigger an unpairing operation to remove a node from a secure domain and return it to the unconnected state.

3.2.18 remote authenticator (RA): Optional function that resides outside the G.hn domain and that may perform some security controller (SC) functions and may control the operation of the SC (e.g., decide which nodes can be authenticated based on pre-specified criteria).

3.2.19 secure admission procedure: Process to establish a secure domain or to include a new node in a secure domain through a standard admission method.

3.2.20 secure domain: Domain where communication between nodes is encrypted.

3.2.21 secure domain master: The domain master of a secure domain.

3.2.22 secure domain name (SDN): The domain name of a secure domain. It shall be different from the default non-secure domain name and the unconnected domain name.

3.2.23 secure endpoint: Any of the endpoints of a secure domain.

3.2.24 secure node: Node that is part of a secure domain.

3.2.25 security controller (SC): Function of a node that manages authentication and key management (AKM) procedures within a G.hn domain.

3.2.26 single-node pairing: Pairing procedure allowing the limitation of the inclusion of new non-secure nodes in a secure domain to one for each run of the procedure. The pairing window closes when one node is authenticated and joins the secure domain.

3.2.27 successful pairing operation: A pairing operation during which a node either creates or joins a secure domain consisting of at least two nodes.

3.2.28 user interface (UI) node: The node connected to a device that allows the user to select which nodes are added or removed to or from a secure domain in a media access control (MAC) authorization operation. It can be selected by using any type of user interface, graphical or not.

3.2.29 unconnected domain name: The domain name used in an unconnected node. It shall be set to "UNCONNECTED".

3.2.30 unconnected node: A non-secure node that does not belong to any domain and that is not connected to any other node.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AE	Application Entity
AKM	Authentication and Key Management
ASCII	American Standard Code for Information Exchange
DM	Domain Master
DN	Domain Name
EP	Endpoint
GUI	Graphical User Interface
LSB	Least Significant Bit
MA	Medium Access
MAC	Media Access Control
MAP	Medium Access Plan
MAP-D	Medium Access Plan-Default
MMPL	Management Message Parameter List
MPDU	Medium access control Protocol Data Unit
MSB	Most Significant Bit
NMK	Network Membership Key
NSD	Non-Secure Domain
PC	Personal Computer
PSDM	Permanent Secure Domain Master
PW	Password
RA	Remote Authenticator
REGID	Registration Identifier
RMAP	Relayed Medium Access Plan
SC	Security Controller
SD	Secure Domain
SDN	Secure Domain Name
TMPDM	Temporal Domain Master
TV	Television

TXOP Transmission Opportunity

UI User Interface

5 Conventions

None.

6 Secure admission methods

An ITU-T G.9961 domain may operate in either non-secure mode or secure mode. Nodes may also be in unconnected state, with the domain name (DN) set as "UNCONNECTED" and not belonging to any domain.

The DN of a non-secure domain (NSD) shall be the default non-secure domain name and the communication is not encrypted. In an NSD, nodes do not need to go through an authentication and key management (AKM) procedure to be admitted (security mode set to zero in Table 8-17 of [ITU-T G.9961]). The DN of all nodes in a secure domain (SD) shall be different from the default NSD and also different from the unconnected DN, and the communication shall be encrypted. In an SD, all the nodes shall go through an AKM procedure to be admitted (security mode set to one in Table 8-17 of [ITU-T G.9961]). The nodes of an SD are configured with a secure domain name (SDN) and password (PW). A PW is a 96-bit parameter as described in clause 9.2.2.2.2 of [ITU-T G.9961] that is used in the G.hn authentication procedure as described in clause 9.2.2.1 of [ITU-T G.9961]. Each joining node that is configured with this SDN and PW can register and be authenticated by the SD. The configured PW enables the registering node to successfully authenticate to the SD. The authentication procedure provides the authenticated node with encryption keys to encrypt or decrypt the data traffic.

The default non-secure domain name is beyond the scope of the Recommendation. SDNs are also beyond the scope of this Recommendation, but they shall not be an empty string and they shall not be the same as the default non-secure domain name or the unconnected domain name. DNs shall be ≤32 characters excluding the NULL string termination character (see Note 1 to Table 8-74 of [ITU-T G.9961]).

NOTE – HomeGrid Forum uses "HomeGrid" as the default non-secure domain name [b-HomeGrid].

A secure node may be configured with an SDN and PW directly by the operator or user, automatically configured during a pairing procedure as specified in clause 6.2.2, or by MAC address authorization as specified in clause 6.1.2.

A node that is configured with an unconnected domain name shall not establish a domain and shall wait in unconnected state until it has been configured with a DN or until it has been admitted to an SD by any secure admission procedure.

The state machine depicted in Figure 6-1 provides a general overview for the basic states of the secure admission protocol.

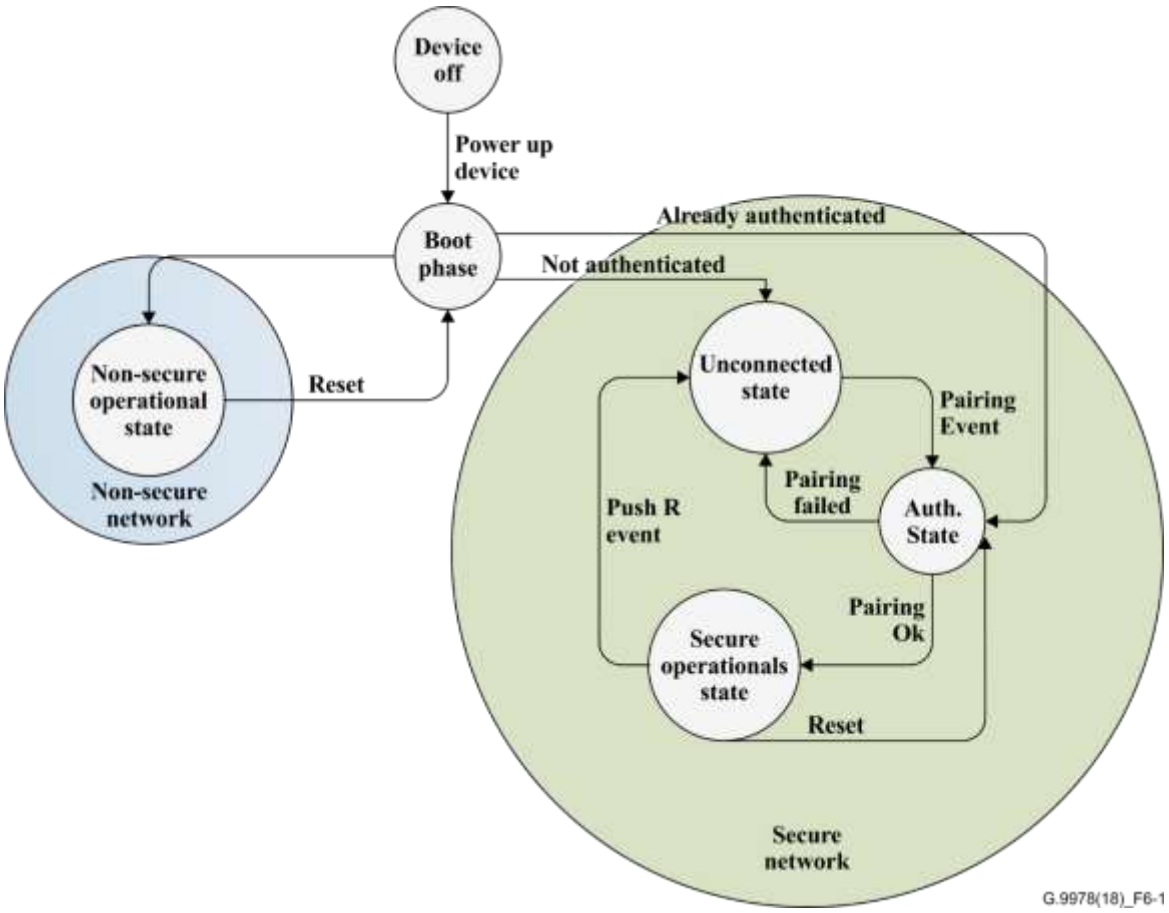

Figure 6-1 – Secure admission state machine

6.1 Media access control authorization-based secure admission procedure

This clause defines a secure admission method based on MAC authorization that enables the user to create a secure G.hn domain and add G.hn devices to an existing secure G.hn domain through an application entity (AE), such as a smart television (TV) or a personal computer (PC).

The mechanisms described in clauses 6.1.1 and 6.1.2 apply to nodes that use the MAC authorization mechanism to get authorized to access the network. Nodes that have already been authorized and therefore have the corresponding encryption keys are not subject to this process and shall be treated as described in clause 8.6.1 of [ITU-T G.9961].

6.1.1 Use cases

This clause describes the use cases for secure admission through MAC authorization, which is based on the comparison of the REGID (MAC address) of the registering node with a list of authorized MAC addresses. See Table 6-1.

Table 6-1 – Use cases for secure admission through MAC authorization

Use Case	Description
1	A user converts a non-secure domain to a new secure domain
2	A user selects one or more nodes in a non-secure domain to establish a secure domain – including the domain master
3	A user selects one or more nodes in a non-secure domain to establish a secure domain – not including the domain master
4	A user adds nodes to an existing secure domain by selecting the nodes from a list displayed on the screen
5	A user adds nodes by configuring information about the new node(s) in the user interface (UI) node
6	A user removes one or more nodes from a domain
7	A user adds nodes by confirming node information of the joining nodes at the user interface node

The use cases described in clauses 6.1.1.1 to 6.1.1.7 depict possible implementations of a graphical user interface (GUI) that assumes that the external GUI is able to discover all the G.hn nodes that are connected to the physical medium. It also assumes that by checking the box, users select the nodes they want to include in a G.hn domain. Nodes for which the user does not check the box are excluded from the domain. This basic GUI is just provided as a guideline for possible implementations.

6.1.1.1 Use case 1 – A user converts a non-secure domain to a new secure domain

In this use case, the user activates an application on the TV screen to display all registered nodes, and selects all the nodes in the list to convert the domain to an SD as illustrated in Figure 6-2.

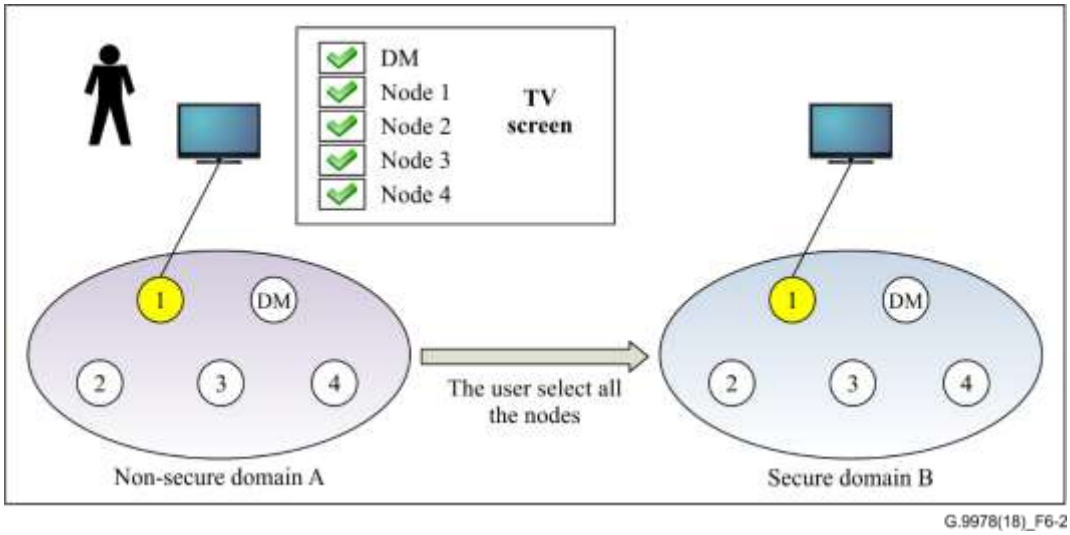

Figure 6-2 – The user converts a non-secure domain to a new secure domain

6.1.1.2 Use case 2 – A user selects one or more nodes in a non-secure domain to establish a secure domain (including the domain master)

In this use case, the user activates an application on the TV screen to display all registered nodes, and selects some of the nodes, including the DM and a number of endpoint (EP) nodes, e.g., the DM, node 1 and node 2 in the list as shown in Figure 6-3, to create a new domain.

NOTE – The user may not know which node is the current DM. This clause covers the case where the DM has been selected. The case that the DM is not selected by the user is described in clause 6.1.1.3.

The remaining nodes that are not selected by the user will run a DM recovery procedure and stay in non-secure mode.

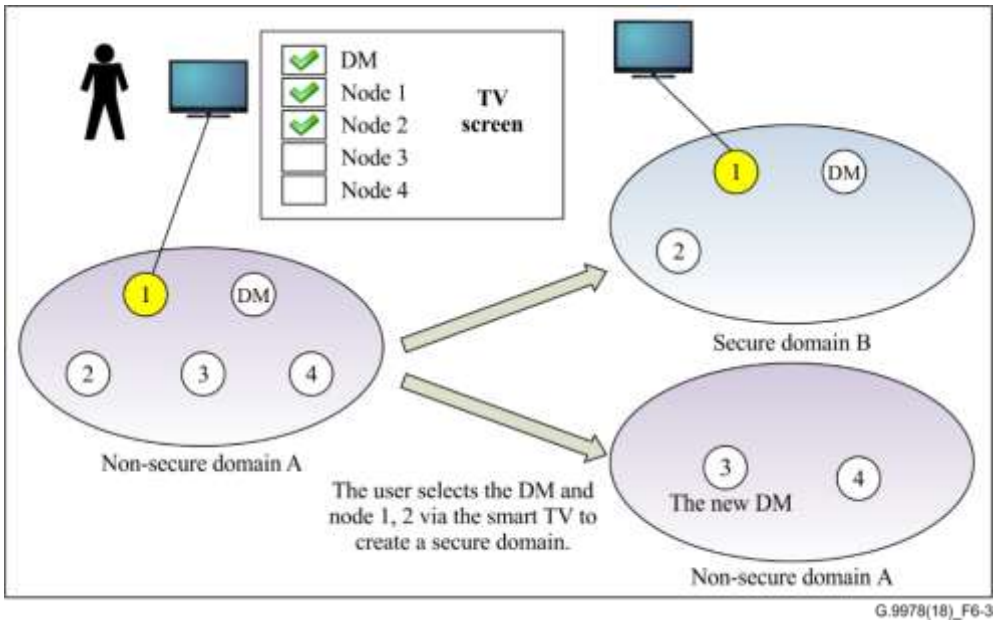

Figure 6-3 – The user selects one or more nodes in a non-secure domain to establish a secure domain (including the domain master)

6.1.1.3 Use case 3 – A user selects a part of the nodes in a non-secure domain to establish a secure domain (not including the domain master)

In this use case, the user activates an application on the TV screen to display all registered nodes, and selects one or more EP nodes, e.g., node 1, 2 and 4 in the list as shown in Figure 6-4, to create a new domain.

The rest nodes that are not selected by the user will stay in the non-secure mode.

NOTE – In use cases 1, 2 and 3, the user interface (UI) node is selected by default**.**

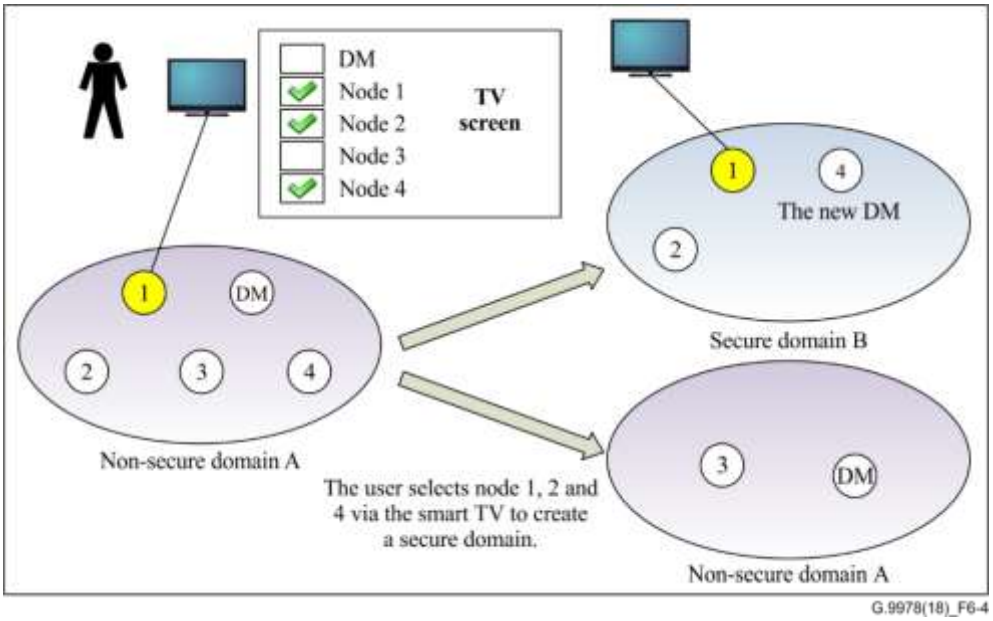

Figure 6-4 – A user selects one or more nodes in a non-secure domain to establish a secure domain (not including the domain master)

6.1.1.4 Use case 4 – A user adds nodes to an existing secure domain by selecting the nodes from a list displayed on the screen

In this use case, the user activates an application on the TV screen to request adding nodes to an SD. The UI node (e.g., the G.hn node that is associated with the smart TV) will collect information about joining nodes and display the list of possible joining nodes on the screen. Then users can select the nodes they want to add and add them to the existing SD.

Figure 6-5 illustrates this use case.

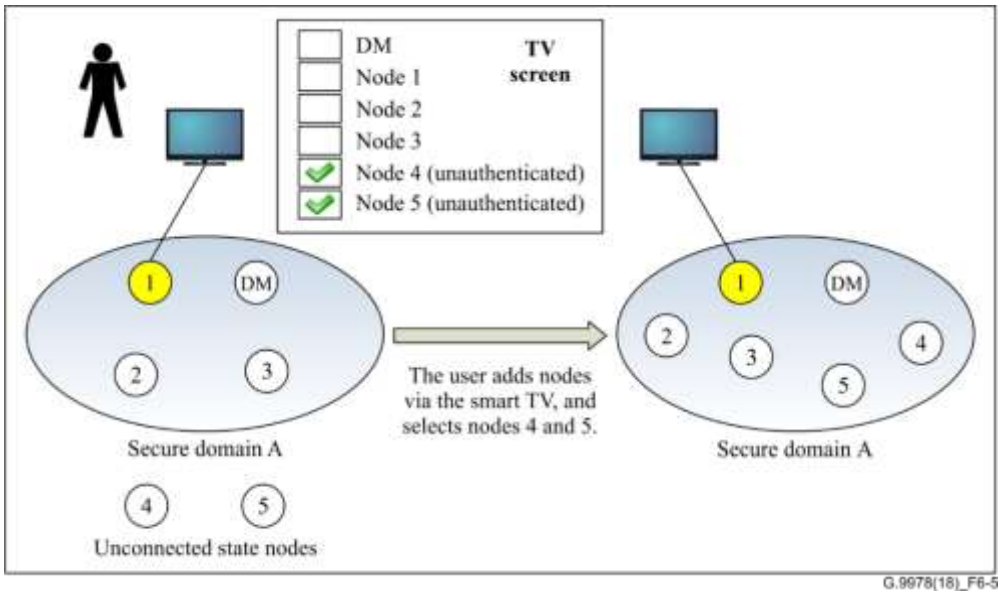

Figure 6-5 – The user adds nodes to an existing secure domain by selecting the nodes from a list displayed on the screen

6.1.1.5 Use case 5 – A user adds nodes by configuring information about the joining node(s) in the user interface node

In this use case, the user can configure information about authorized joining nodes in the UI node (e.g., via the webpage), and the UI node will convey the information to the DM. The DM will then allow the registration of these nodes. Figure 6-6 illustrates this use case.

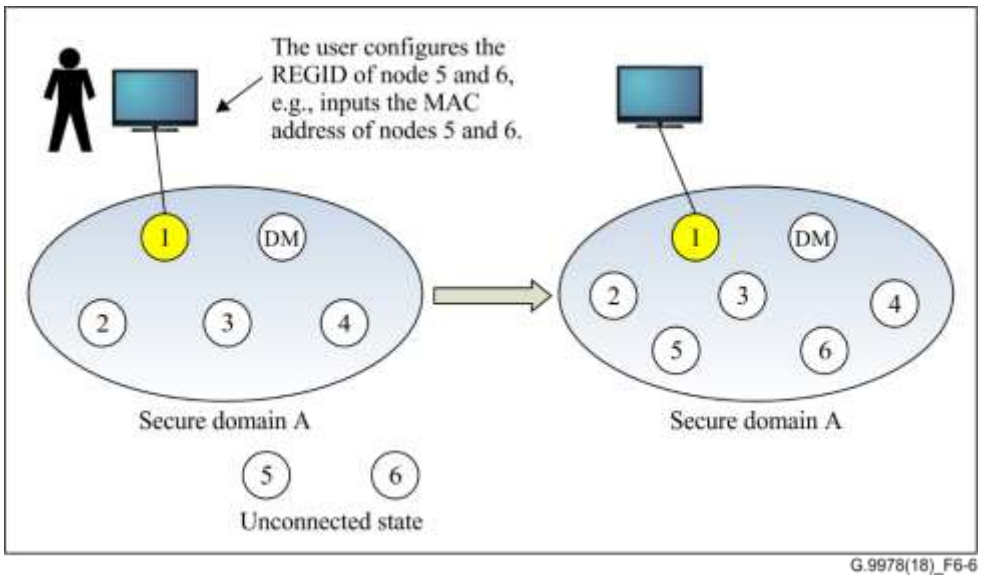

Figure 6-6 – The user adds nodes by configuring information about the joining node in the user interface node

6.1.1.6 Use case 6 – A user removes one or more nodes from a domain

In this use case, the user activates an application on the TV screen to display all registered nodes, and selects the EP nodes he wants to remove from the domain. Figure 6-7 illustrates this use case.

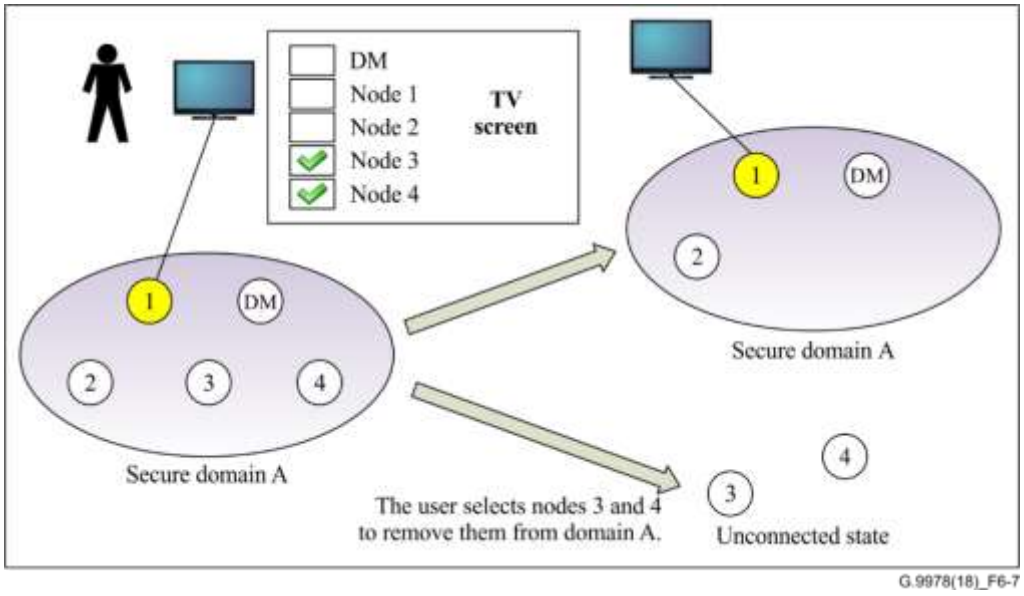

Figure 6-7 – The user removes one or more nodes from a secure domain

6.1.1.7 Use case 7 – A user adds nodes by confirming the node information of the joining nodes at the user interface node

In this case, when the new node first powers on, it broadcasts a message to notify the network of its existence. When the DM receives the message, it will notify the UI node of the existence of the new node, and the AE will pop up a message on the TV screen indicating that the new node exists and asking if the new node is allowed to join the secure domain. The new node is allowed to join the secure domain if the user authorizes it to do so.

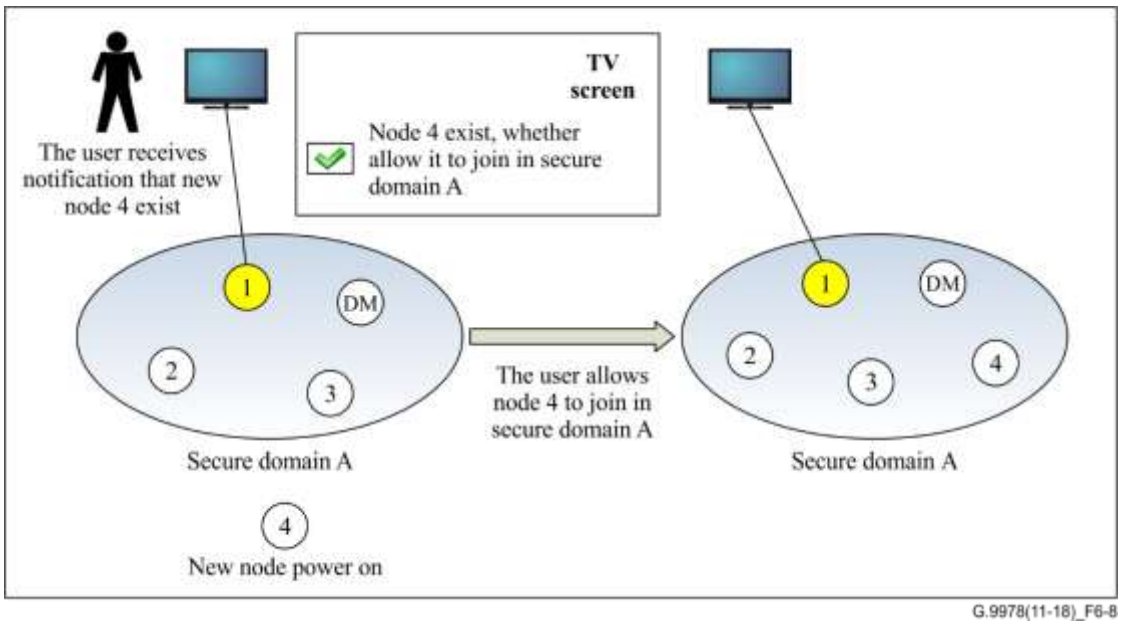

Figure 6-8 – AE pops up a message on the TV screen to notify of the existence of a new node, and the user chooses to whether allow it join the secure domain or not

NOTE – Other nodes in the neighbourhood may also receive the notification message, and pop up the message on the TV screen. Vendors should implement vendor discretionary means to avoid security issues related to this.

6.1.2 Secure admission description

The user may use an AE to secure an NSD, to include new nodes in an existing SD and to remove nodes from an existing SD.

6.1.2.1 Secure admission protocol for creating a secure domain

In order to convert an NSD to an SD or create an SD via an AE that shows all registered nodes, users shall select the nodes that they wish to add to the SD.

The application shall send the list of the authorized nodes, composed of the nodes that are selected by the user to create an SD, to the attached G.hn node (i.e., the UI node).

If the UI node is not included in the list of authorized nodes, the procedure shall be aborted and an error message presented to the user.

If the DM is included in the list of authorized nodes (see clauses 6.1.1.1 and 6.1.1.2), the UI node shall send an ADM_UI_MACauthorization.req message to its DM. The ADM_UI_Pairing.req message shall include the list of the authorized nodes' MAC addresses selected by the user.

On receipt of an ADM_UI_MACauthorization.req message, the DM shall reply with an ADM_UI_MACauthorization.cnf message to the UI node within 100 ms, and then generate a SDN and a PW and send an ADM_SecureDomain.req message to all authorized registered nodes in the domain to inform them that the domain has converted into an SD. The ADM_SecureDomain.req message shall include the newly generated SDN, the PW for authentication and the SC REGID.

If the UI node does not receive an ADM_UI_MACauthorization.cnf message from the DM within 200 ms, the UI node shall repeat the request. If, after the second request, the proxy node still does not receive the ADM_UI_MACauthorization.cnf message within 200 ms, the request to create an SD fails.

On receipt of the ADM_SecureDomain.req message, the receiving node shall confirm receipt by replying with an ADM_SecureDomain.cnf message within 100 ms. The receiving node shall adopt the new SDN and PW.

After the DM receives ADM_SecureDomain.cnf message from all its addressed nodes, or a 200 ms timeout expires, it shall start to transmit the medium access plan (MAP) with the new SDN.

On receipt of the MAP with the new SDN, each node shall start the authentication procedure specified in [ITU-T G.9961].

NOTE 1 – The nodes that are not included in the list of authorized nodes shall stay in non-secure mode, and they may perform the DM recovery procedure as specified in clause 8.6.6.2 of [ITU-T G.9961].

The protocol diagram of the secure admission for use case 1 and 2 is presented in Figure 6-9.

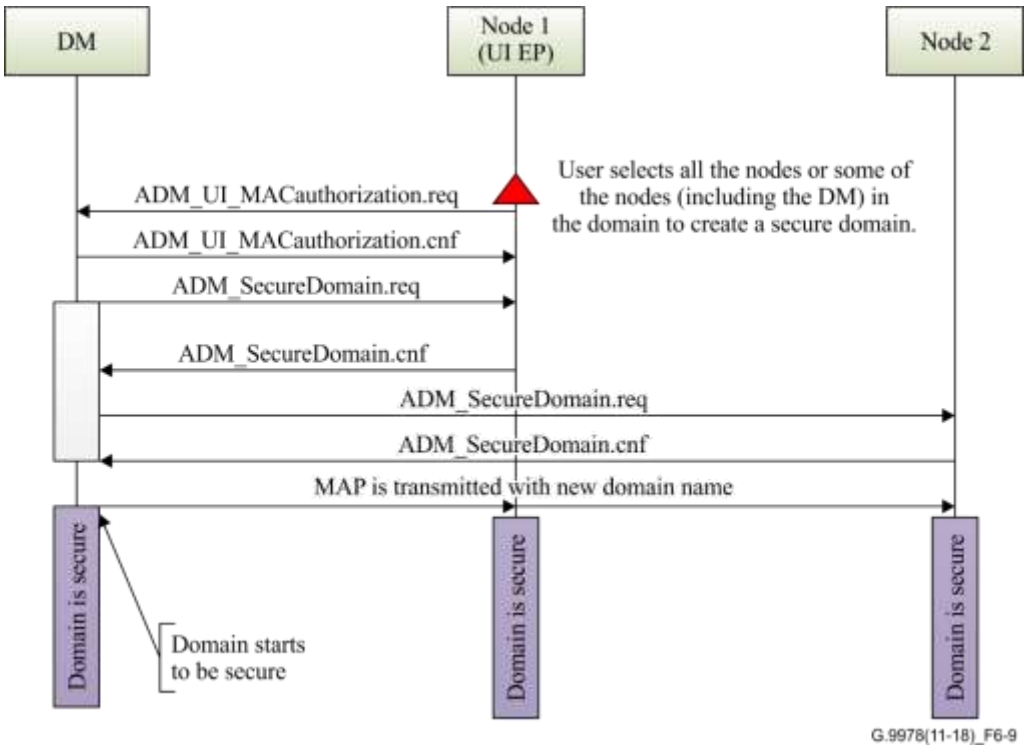

Figure 6-9 – Protocol diagram describing secure admission for use case 1 and 2

If the DM is not included in the list of authorized nodes (see clause 6.1.1.3), the UI node shall send an ADM_UI_MACauthorization.req message to all the nodes in the list. After receipt of the list of authorized nodes, every authorized node shall reply to the UI node within 200 ms with an ADM_UI_MACauthorization.cnf message and then rank its DM capabilities based on the criteria as specified in clause 8.6.6.3 of [ITU-T G.9961]. The highest ranking authorized node shall become a new DM of a new SD by generating a random SDN and a PW and start transmitting MAPs with the generated DN.

The authorized node that detects the MAP or relayed medium access plan (RMAP) of an SD from one of the authorized nodes shall register in the new DM within 1 s and the new DM shall send them the PW for authentication if it accepts their registration request. After 1 s, the new DM shall stop the registration of these authorized nodes.

If an authorized node fails to detect the MAP from the highest ranking authorized node after a 1 s timeout, it shall return to the state it was before it received the ADM_UI_MACauthorization.req message from the UI node, which could be an unconnected state or a non-secure operational state.

NOTE 2 – Whether the DM is selected by the user or not, the UI node shall be selected by default and become the SC of the new SD.

Figure 6-10 is the protocol diagram of the secure admission for use case 3.

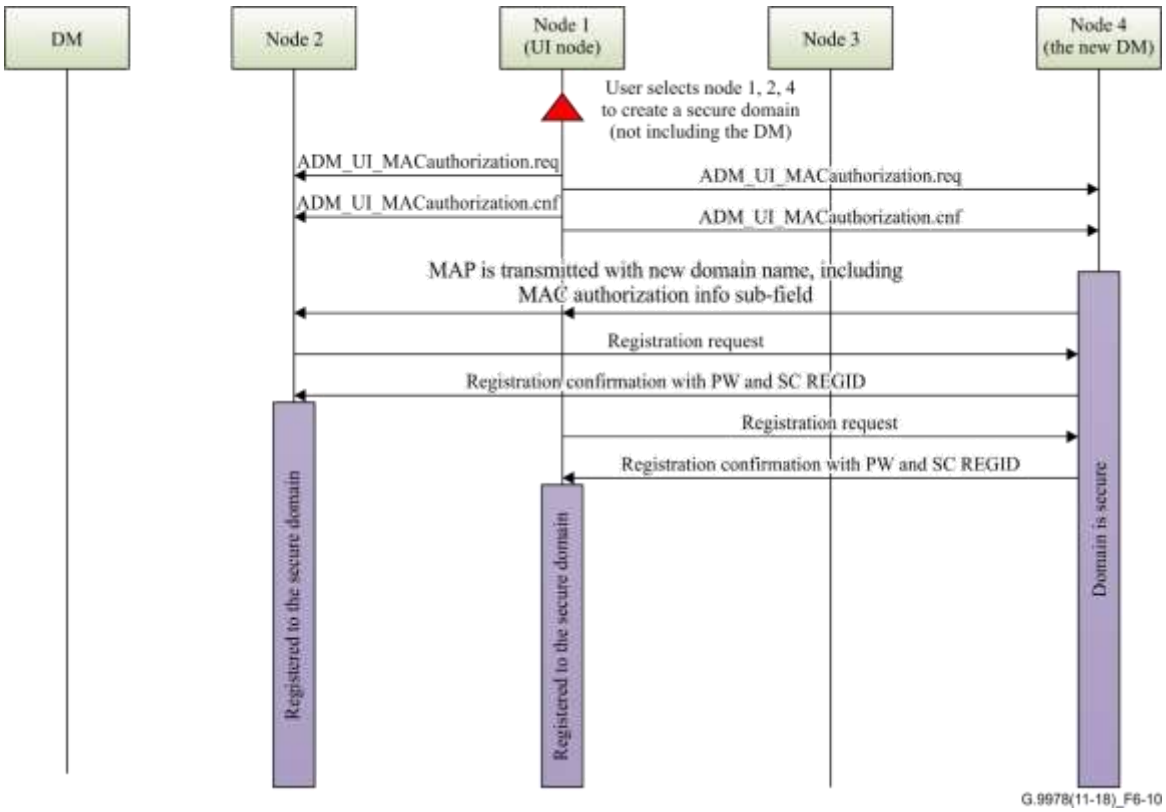

Figure 6-10 – Protocol diagram describing secure admission for use case 3

6.1.2.2 Secure admission protocol for adding nodes to an existing secure domain

Users may add new nodes to an existing SD by:

– activating an application on the AE to request adding nodes and selecting the nodes they wish to include in this SD in a list (see clause 6.1.1.4), or

– configuring the information (e.g., inputting the MAC addresses) of the nodes they wish to include via the UI node (see clause 6.1.1.5).

6.1.2.2.1 Adding nodes by user selection

If the user activates an application to request adding nodes to an SD, the AE shall trigger the attached G.hn node (i.e., the UI node) to send an ADM_UI_MACauthorization.ind message to the DM. If the UI node is the SC of this SD or it has been authorized by the SC, it can send the ADM_UI_MACauthorization.ind message directly. If the proxy node has not been authorized by the SC, the UI node shall request authorization by the SC before it sends the ADM_UI_MACauthorization.ind message to the DM. In order to get authorized by the SC, the UI node shall send the SC a SC_UI_Authorization.req message, which shall be encrypted using the NSC key. The SC shall reply with an SC_UI_Authorization.cnf message to the UI node to indicate whether the request is accepted. If the SC accepts the authorization request from the UI node, it shall send a SC_UI_Authorization.ind message to the DM to inform the UI node of the authorization.

After receiving the indication message, the DM shall open a window to allow registration of the nodes that do not have the PW, only if it has already received the SC_UI_Authorization.ind message from the SC indicating that the UI node has been authorized. During this time window, the DM shall broadcast the MAP frames with the RegistrationOffer field set to one. The nodes in unconnected states that can detect the MAP or RMAP frames from this SD shall register in the DM. The DM shall send the list of these nodes to the UI node by sending an ADM_UI_MACauthorization.rsp message when the time window expires. Besides these nodes, the DM shall also include information about neighbouring nodes that have been detected from an NSD in an ADM_UI_MACauthorization.rsp message.

NOTE – The DM collects information about neighbouring nodes, including the REGID and DN as specified in [ITU-T G.9961].

After receiving the ADM_UI_MACauthorization.rsp message, the AE associated with the UI node displays the list of nodes in this message on the screen. Users can then select the nodes they wish to add. The application shall send the list of authorized nodes selected by the user to the attached G.hn node, which will trigger the UI node to send an ADM_UI_MACauthorization.req message to the DM. The "RequestReason" field of the ADM_UI_MACauthorization.req message shall be set to 3_{16}.

On receipt of the ADM_UI_MACauthorization.req message, the DM shall reply to the UI node within 100 ms with an ADM_UI_MACauthorization.cnf message and then send an ADM_SecureDomain.req message, which includes the PW for authentication, to the authorized nodes that have registered on it. The DM shall also distribute an MAC authorization information subfield to the Medium Access Plan-Default (MAP-D) frames for 120 s, which includes collected information about neighbouring nodes that have registered in an NSD. A node in an NSD shall monitor MAP-D frames from neighbouring domains and, if it detects that its information is included in the MAC authorization information subfield in the MAP-D frames, it shall leave the NSD and register in the SD.

On receipt of the ADM_SecureDomain.req message, the receiving node shall confirm receipt by replying with an ADM_SecureDomain.cnf message within 100 ms. The receiving node shall use the PW and DN to complete authentication with the SC. The nodes that are not selected by the user shall be rejected by the DM.

If a node in an NSD detects a MAP-D or RMAP-D frame from an SD that includes its information in the MAC authorization subfield, it shall try to register in the SD. If the DM of this SD receives the registration request from this node, it shall send the PW in the registration confirmation to this node.

Figure 6-11 is the protocol diagram of the secure admission for use case 4.

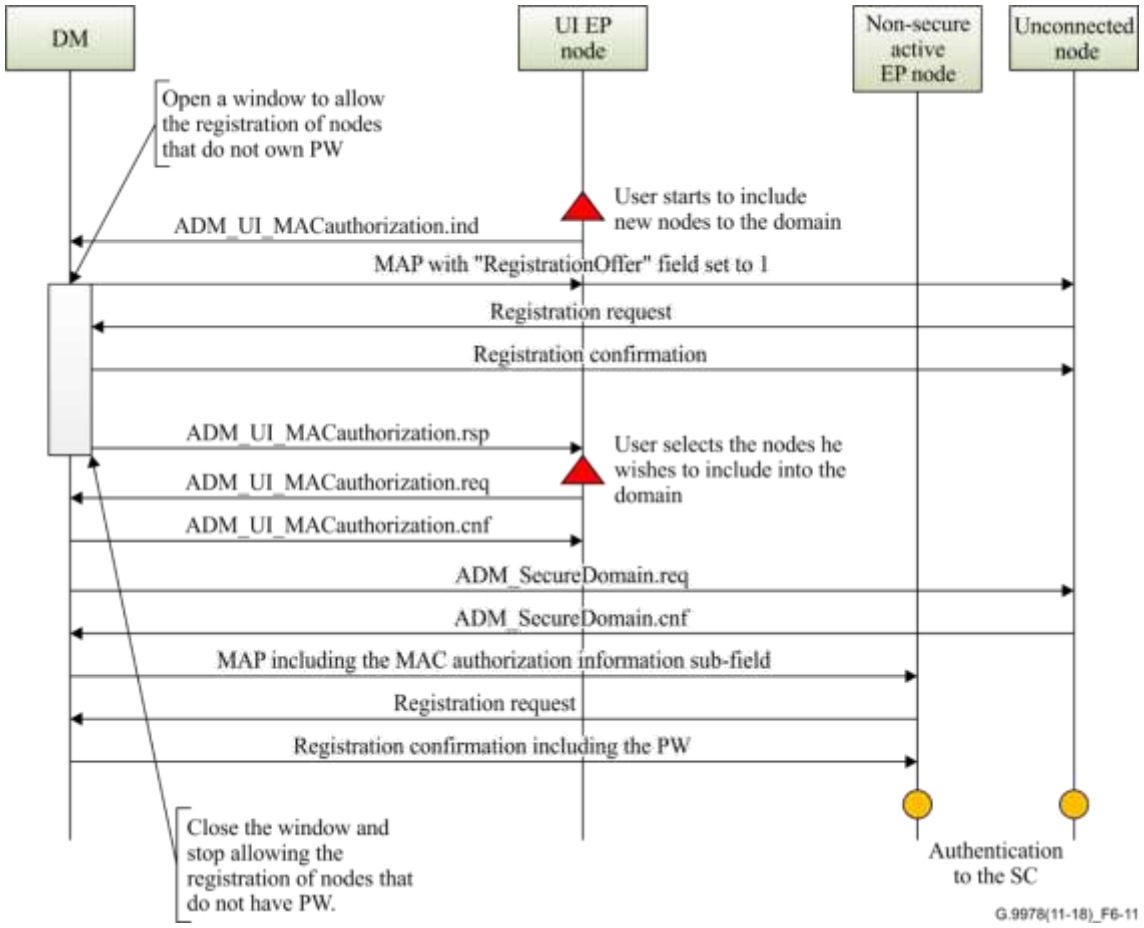

Figure 6-11 – Protocol diagram describing secure admission for use case 4

6.1.2.2.2 Adding nodes by user configuration

If users configure the information (i.e., input the MAC address) of the nodes they wish to include in the existing domain on the AE that is associated with the G.hn UI node, the AE shall trigger the attached G.hn node (i.e., the UI node) to send an ADM_UI_MACauthorization.req message to its DM. The ADM_UI_MACauthorization.req message shall include the list of the MAC addresses of the authorized nodes input by the user and the "RequestReason" field shall be set to 4_{16}.

If the UI node is the SC of this SD or it has been authorized by the SC, it can send the ADM_UI_MACauthorization.req message directly. If the UI node has not been authorized by the SC, the UI node shall request to be authorized by the SC before it sends the ADM_UI_MACauthorization.req message to the DM. In order to get authorized by the SC, the UI node shall send the SC a SC_UI_Authorization.req message, which shall be encrypted using the NSC key. The SC shall reply with an SC_UI_Authorization.cnf message to the UI node to indicate whether the request is accepted. If the SC accepts the authorization request from the UI node, it shall send an SC_UI_Authorization.ind message to the DM to inform the UI node of the authorization.

On receipt of the ADM_UI_MACauthorization.req message, the DM shall reply to the UI node within 100 ms with an ADM_UI_MACauthorization.cnf message only if it has already received the ADM_UI_Authorization.ind message from the SC indicating that the UI node has been authorized. The DM shall then include a MAC authorization information auxiliary subfield in the MAP-D frames, which includes information about the authorized nodes in the list. During 120 s, only the authorized nodes and the nodes that have a valid PW are allowed to register in the new SD.

When a node detects an MAP-D or RMAP-D frame that includes the MAC authorization information auxiliary subfield, it shall check whether it is included in this auxiliary subfield. If its MAC address matches the information in this auxiliary subfield, it shall send the registration request to the DM according to the registration procedure specified in [ITU-T G.9961]. On receipt of the registration message from an authorized node, the DM shall also check whether the registering node is an authorized node, the DM shall send the authorized registering node an ADM_DmRegistrResponse.cnf message including the PW for authentication and reject the registration request from any node that is not included in the authorized nodes.

After 120 s, the DM shall remove the MAC authorization information auxiliary subfield from the MAP-D frame and stop allowing the registration of these authorized nodes.

Figure 6-12 is the protocol diagram of the secure admission for use case 5.

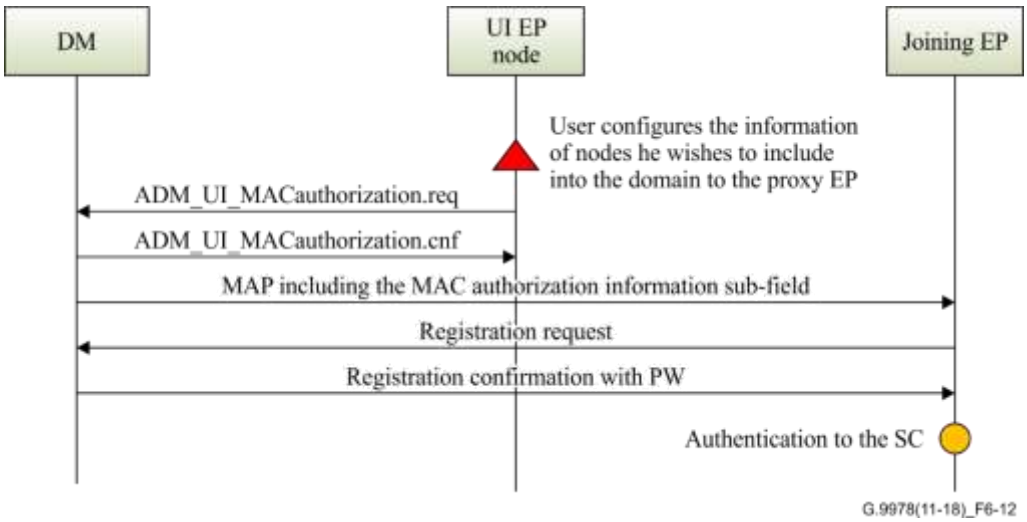

Figure 6-12 – Protocol diagram describing secure admission for use case 5

6.1.2.2.3 Adding nodes by user confirmation

If a new node powers on in the home network, it will broadcast an ADM_SelfNotify.ind message with its REGID "A" to notify of its existence. When the DM receives this ADM_SelfNotify.ind message, it sends an ADM_UINewNodeExist.ind message with REGID "A" to the UI node. The AE that is associated with G.hn UI node will pop up a message with REGID "A" to let the user know that a new node is joining the network. If the user accepts that the new device can join the secure domain, the UI node shall send an ADM_UI_MACauthorization.ind message to the DM.

After receiving the indication message, the DM shall open a window to allow registration of this node with REGID "A", only if it has already received the SC_UI_Authorization.req message from the SC indicating that the UI node has been authorized. During this time window, the DM shall broadcast the MAP frames with the RegistrationOffer field set to two and the "RegistratioRestrict" field set to REGID "A". The nodes that work with REGID "A" shall register in the DM.

After the new unconnected node receives the registration confirmation message, it shall send an ADM_SecureDomain.req message, which includes the PW for authentication, to the authorized nodes that have registered on it. The DM shall also distribute a MAC authorization information subfield to the Medium Access Plan-Default (MAP-D) frames for 120 s, which includes collected information about neighbouring nodes that have registered in an NSD. A node in an NSD shall monitor MAP-D frames from neighbouring domains and, if it detects that its information is included in the MAC authorization information subfield in the MAP-D frames, it shall leave the NSD and register in the SD.

On receipt of the ADM_SecureDomain.req message, the receiving node shall confirm receipt by replying with an ADM_SecureDomain.cnf message. The receiving node shall use the PW and DN to complete authentication with the SC. The nodes that do not work with REGID "A" shall be rejected by the DM.

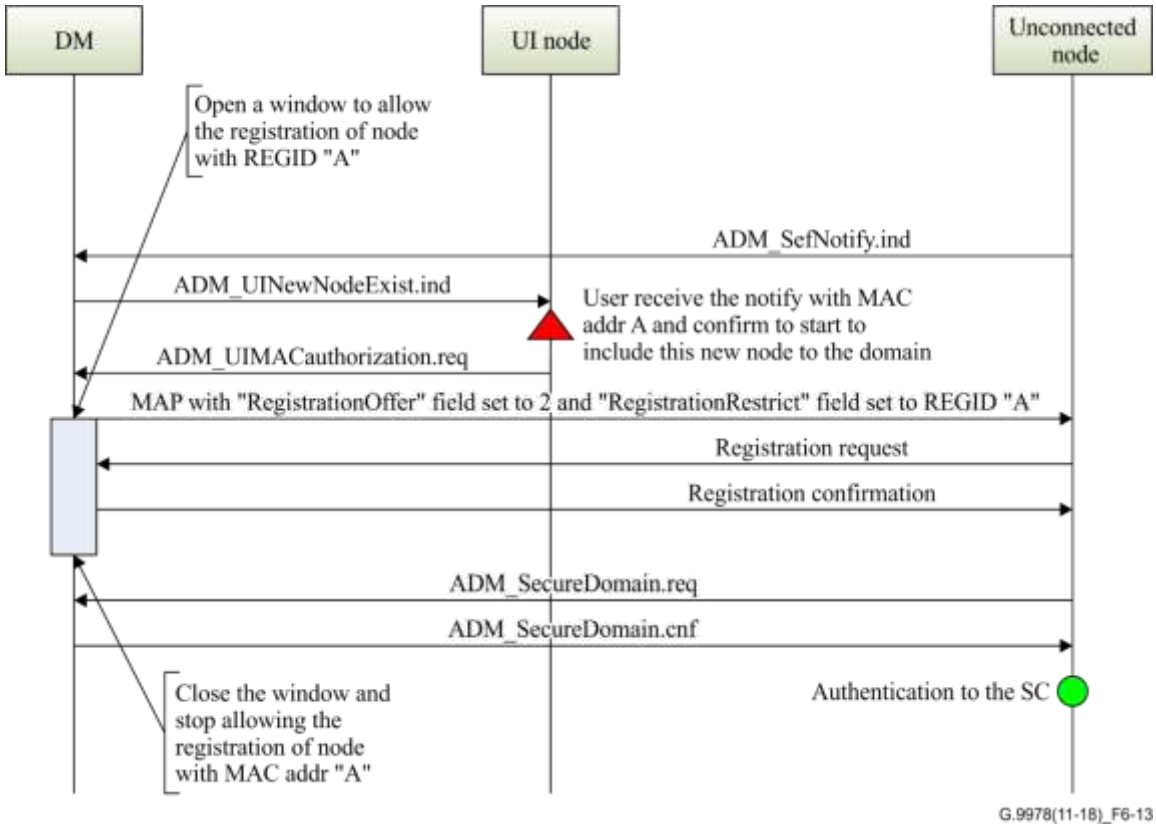

Figure 6-13 – Protocol diagram describing secure admission for use case 7

6.1.2.3 Removing nodes from a domain through MAC authorization

Users may remove nodes through the AE that shows them the registered nodes. Users select the nodes that they wish to remove from the domain. The application shall send the list of the nodes to be removed to the attached G.hn node and trigger the node to send an ADM_UI_MACauthorization.req message to its DM. The ADM_UI_MACauthorization.req message shall include the list of the authorized nodes' MAC Address selected by the user and the "RequestReason" field shall be set to 5_{16}.

On receipt of the ADM_UI_MACauthorization.req message, the DM shall reply to the UI node within 100 ms with an ADM_UI_MACauthorization.cnf message and then force the resignation of the nodes in the received ADM_UI_MACauthorization.req message according to the procedure specified in [ITU-T G.9961].

6.1.2.4 MAC authorization secure admission protocol messages

The following clauses specify the messages to support the MAC authorization secure admission protocol.

6.1.2.4.1 Format of ADM_UI_MACauthorization.req

The ADM_UI_MACauthorization.req message shall be sent by the UI node to the DM or other EP nodes to convey list of the authorized nodes during the MAC authorization secure admission process.

The format of the management message parameter list (MMPL) of the ADM_UI_MACauthorization.req message shall be as shown in Table 6-2.

Table 6-2 – Format of the management message parameter list of the ADM_UI_MACauthorization.req message

Field	Octet	Bits	Description
RequestReason	0	[3:0]	0_{16}: Convert a non-secure domain to a secure domain 1_{16}: Select some of the nodes to create a secure domain (including the DM) 2_{16}: Select some of the nodes to create a secure domain (not including the DM) 3_{16}: Include nodes to a secure domain according to the user's selection 4_{16}: Include nodes to a secure domain by configure the info of these nodes 5_{16}: Remove nodes from a domain 6_{16}: Include a node with a specific REGID in a secure domain after confirmation from the user 7_{16}-F_{16} – Reserved by ITU-T
Reserved		[7:4]	Reserved by ITU-T (Note)
NumAuthNodes	1	[7:0]	The number of authorized nodes
REGID1	2 to 7	[47:0]	The REGID of the first authorized node
…	…	…	…
REGIDN	Var	[47:0]	The REGID of the *N*th authorized node
NOTE – Bits that are reserved by ITU-T shall be set to zero by the transmitter and ignored by the receiver.			

6.1.2.4.2 Format of ADM_UI_MACauthorization.cnf

The ADM_UI_MACauthorization.cnf message shall be sent by the DM or EP nodes to the UI nodes to confirm receipt of the ADM_UI_MACauthorization.req message.

The MMPL of the ADM_UI_MACauthorization.cnf message is empty.

6.1.2.4.3 Format of ADM_SecureDomain.req

The ADM_SecureDomain.req message shall be sent by the DM to the authorized node to convey the PW and other parameters of the domain for authentication.

The format of the MMPL of the ADM_SecureDomain.req message shall be as shown in Table 6-3.

Table 6-3 – Format of the MMPL of the ADM_SecureDomain.req message

Field	Octet	Bits	Description
DomainName	0 to 31	[255:0]	This field shall indicate the 32-octet domain name represented in American standard code for information exchange (ASCII) characters (Note)
Password	32 to 43	[95:0]	This field shall include the user password for node authentication for this domain name
SCRegID	44 to 51	[47:0]	This field shall include the REGID of the SC of the domain

NOTE – The ASCII characters shall be mapped on to the bytes of the domain name in the following way:

– the least significant bit (LSB) of the 7-bit ASCII character is mapped on to bit b0 of the corresponding byte of the domain name;

– the most significant bit (MSB) of all bytes shall be set to zero;

– the first ASCII character of the domain name shall be mapped on to the least significant byte of the domain name (e.g., if the domain name is "Network", the first ASCII character is letter "N" that shall be mapped at byte 0 of the domain name);

– if the number of provided ASCII characters is less than 32, the rest of the domain name field bytes shall be set to 00_{16}.

6.1.2.4.4 Format of ADM_SecureDomain.cnf

The ADM_SecureDomain.cnf message shall be sent by the joining node in response to an ADM_SecureDomain.req message.

The MMPL of the ADM_SecureDomain.cnf message is empty.

6.1.2.4.5 Format of ADM_UI_MACauthorization.ind

The ADM_UI_MACauthorization.ind message shall be sent by the UI node to the DM to report that the user wishes to include nodes in the domain. The DM shall then open a registration window to allow the registration of the nodes that do not have the PW.

The MMPL of the ADM_UI_MACauthorization.ind message is empty.

6.1.2.4.6 Format of ADM_UI_MACauthorization.rsp

The ADM_UI_MACauthorization.rsp message shall be sent by the DM to the UI node in response to the ADM_UI_MACauthorization.ind message to provide information about the registered node(s) that do not have the PW.

The format of the MMPL of the ADM_UI_MACauthorization.rsp message shall be as shown in Table 6-4.

Table 6-4 – Format of the MMPL of the ADM_UI_MACauthorization.rsp message

Field	Octet	Bits	Description
NumNodes	0	[7:0]	The number of the nodes that the DM collects for the user to select
NodeRegID1	1	[47:0]	The REGID of the first node
…	…	…	…
NodeRegIDN	Var	[47:0]	The REGID of the *N*th node

6.1.2.4.7 Format of SC_UI_Authorization.req

The SC_UI_Authorization.req message shall be sent by a node to the SC to request to be authorized as the UI node for MAC authorization-based secure admission.

The format of the MMPL of the SC_UI_Authorization.req message shall be as shown in Table 6-5.

Table 6-5 – Format of the MMPL of the SC_UI_Authorization.req message

Field	Octet	Bits	Description
DeviceID	0	[7:0]	The DEVICE_ID of the node requesting to be authorized as the UI node
RegID	1-6	[47:0]	The REGID of the node requesting to be authorized as the UI node
NumAuthNodes	7	[7:0]	The number of the nodes authorized by the user
RegID1	8 to 13	[47:0]	The REGID of the first authorized node
…	…	…	…
RegIDN	Var	[47:0]	The REGID of the *N*th authorized node

6.1.2.4.8 Format of SC_UI_Authorization.cnf

The SC_UI_Authorization.cnf message shall be sent by the SC in response to the received SC_UI_Authorization.req message.

The format of the MMPL of the SC_UI_Authorization.cnf message shall be as shown in Table 6-6.

Table 6-6 – Format of the MMPL of the SC_UI_Authorization.cnf message

Field	Octet	Bits	Description
StatusCode	0	[7:0]	Value that indicates whether or not the request has been accepted by the SC: 00_{16} = Success (the request is accepted) 01_{16} = Failure (no reason provided) 02_{16}-FF_{16} = Reserved by ITU-T

6.1.2.4.9 Format of SC_UI_Authorization.ind

The SC_UI_Authorization.ind message shall be sent by the SC to the DM to report that an EP node has been authorized as a UI node for MAC authorization-based secure admission.

The format of the MMPL of the SC_UI_Authorization.ind message shall be as shown in Table 6-7.

Table 6-7 – Format of the MMPL of the SC_UI_Authorization.ind message

Field	Octet	Bits	Description
DeviceID	0	[7:0]	The DEVICE_ID of the node requesting to be authorized
RegID	1-6	[47:0]	The REGID of the node requesting to be authorized

6.1.2.4.10 Format of ADM_SelfNotify.ind

The ADM_SelfNotify.ind message will be broadcast to the network by a new unconnected node to notify of its existence and inform of its REGID.

The format of the management message parameter list (MMPL) of the ADM_SelfNotify.ind message shall be as shown in Table 6-8.

Table 6-8 – Format of the management message parameter list of the ADM_SelfNotify.ind message

Field	Octet	Bits	Description
REGID	6	[47:0]	REGID (MAC address) of the new node

6.1.2.4.11 Format of ADM_UINewNodeExist.ind

The ADM_UINewNodeExist.ind message shall be sent by the DM to the UI node to convey the REGID of the new unconnected node.

The format of the management message parameter list (MMPL) of the ADM_UINewNodeExist.ind message shall be the same as that of the ADM_SelfNotify.ind message, as shown in Table 6-8.

6.2 Admission through generic pairing mechanism

This clause defines a secure admission method that enables establishment of an SD that requires minimal user intervention and avoids the use of a computer to configure a secure G.hn network. This kind of mechanism is commonly known as push-button security (or pairing) and is already available in many existing home networking technologies. This pairing method addresses special requirements that are derived from the special characteristics of G.hn domains. This pairing mechanism supports two pairing modes: single-node pairing mode, to add a single non-secure node to a SD per pairing operation; and multi-node pairing mode that enables several non-secure nodes to enter the SD during the same pairing window. A G.hn domain may work exclusively in only one mode. The pairing mechanism in single-node mode and in multi-node pairing mode shall address the use cases that are specified in clause 6.2.1. When more than one button needs to be pushed, the order of pushing these buttons is irrelevant.

The mechanisms described in clauses 6.2.1 and 6.2.2 apply to nodes that use the generic pairing mechanism to get authorization to access the network. Nodes that have already been authenticated and therefore have the corresponding encryption keys are not subject to this process and shall be treated as described in clause 8.6.1 of [ITU-T G.9961] (i.e., they will be accepted even if the pairing window is closed).

6.2.1 Use cases

Clauses 6.2.1.1 to 6.2.1.10 describe the behaviour of the different nodes of a domain in different situations. See Table 6-9.

Table 6-9 – Use cases for secure admission through a push-button mechanism

Use case	Description	Comments
1-a	Single-node pairing mode – Convert a non-secure domain to a new secure domain through generic pairing	
1-b	Single-node pairing mode – Add a node in an unconnected state to a secure domain	
2-a	Single-node or multi-node pairing mode – Add a node from a non-secure domain to an existing secure domain	
2-b	Single-node or multi-node pairing mode – Add a node that is in an unconnected state to an existing secure domain	
3	Single-node or multi-node pairing mode – A node that was already paired is switched off and switched on again	
4	Single-node or multi-node pairing mode. Power up of a node that is configured with unconnected domain name	
5	Multi-node pairing mode – Convert a non-secure domain into a secure domain	
6	Multi-node pairing mode – Add multiple nodes from a default domain or in unconnected state into a secure domain	
7-a	Fault case – Single-node or multi-node pairing mode – User sends only the PUSH_P event on one node of a non-secure domain	
7-b	Fault case – Single-node or multi-node pairing mode – User sends only the PUSH_P event on one node that is in an unconnected state	
8	Fault case – Single-node or multi-node pairing mode – User sends the PUSH_P only on one node in a secure domain	
9	Fault case In single-node pairing mode – User tries to add two nodes within one pairing window	
10	PUSH_R case – User triggers PUSH_R event on a node in a secure domain	
11	Single node pairing by user confirmation	

6.2.1.1 Use case 1-a – Convert a non-secure domain to a secure domain through generic pairing

This use case refers to single-node pairing mode, it includes a deployment of nodes that were installed at a home as an NSD with a default non-secure domain name (after power up, the nodes may be configured to create an NSD with a default non-secure domain name).

After this NSD is established, the user can convert the NSD to an SD by the generic pairing procedure.

Through push button mechanism, the user adds nodes to the domain one by one. Each pairing procedure adds a node to the domain

The user sends the PUSH_P event to two nodes in the NSD. As a result, the two nodes establish a new SD, with a new SDN as illustrated in Figure 6-14 (Step 1).

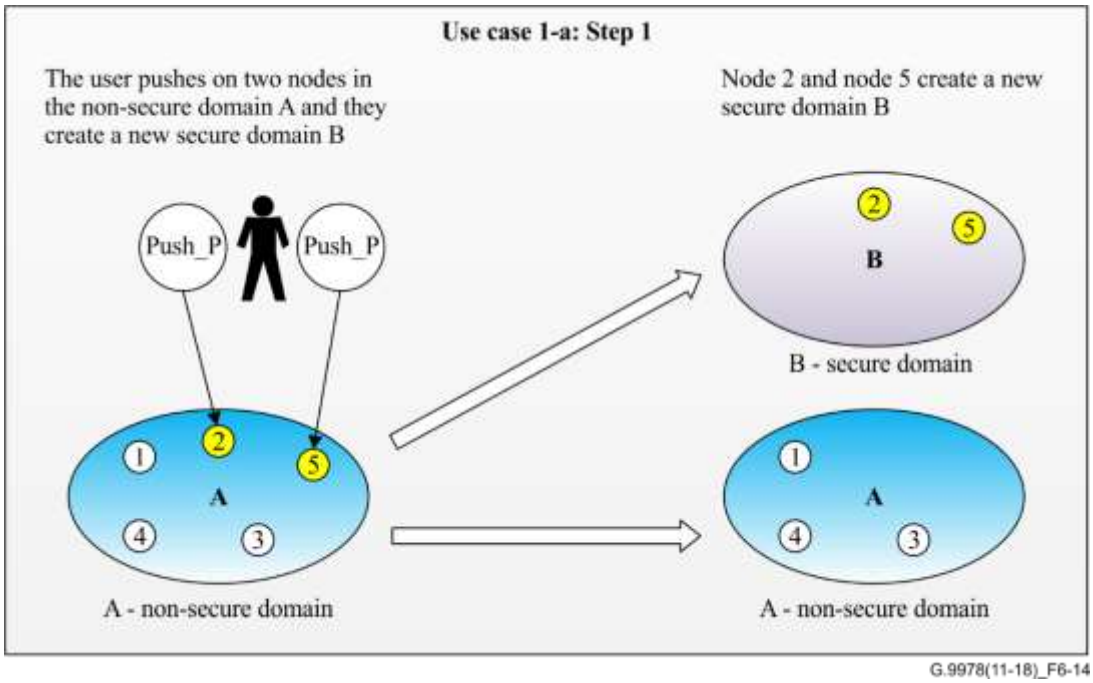

Figure 6-14 – Use case 1-a: Step 1 – User converts a non-secure domain to a secure domain

In order to convert the entire NSD to an SD, the user has to continue the generic pairing procedure by triggering the push button event in each node of the NSD and in one of the nodes from the SD as illustrated in Figure 6-15 (Step 2).

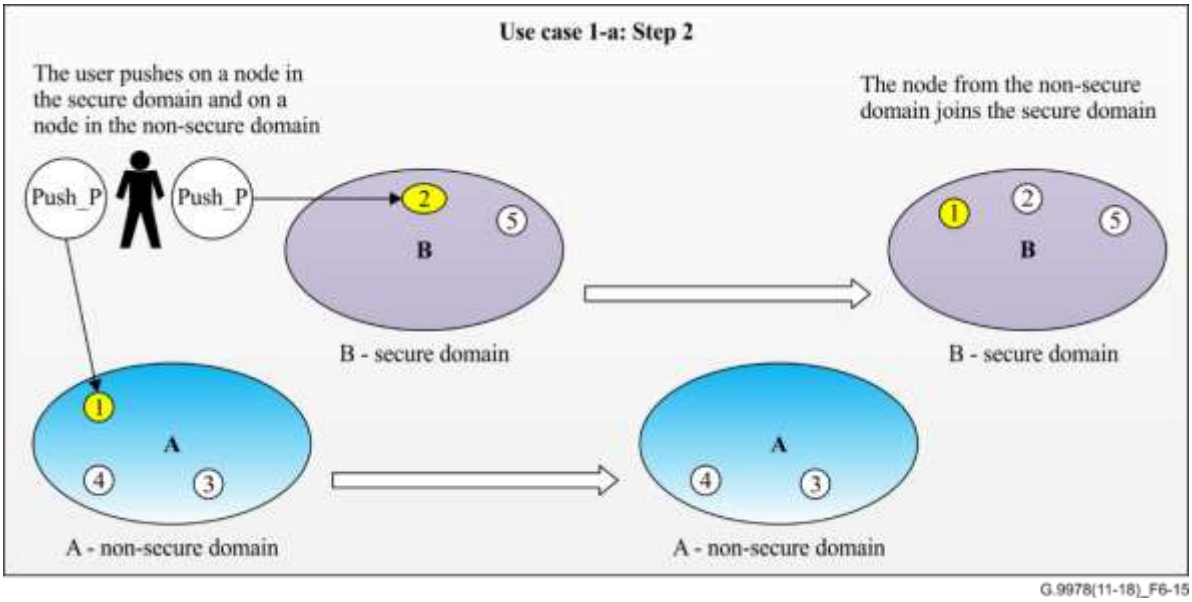

Figure 6-15 – Use case 1-a: Step 2 – The user removes a node from the non-secure domain to the secure domain

After the user runs the generic pairing procedure with the last node in the NSD, the last node is added to the SD and the NSD disappears as illustrated in Figure 6-16 (Step 3).

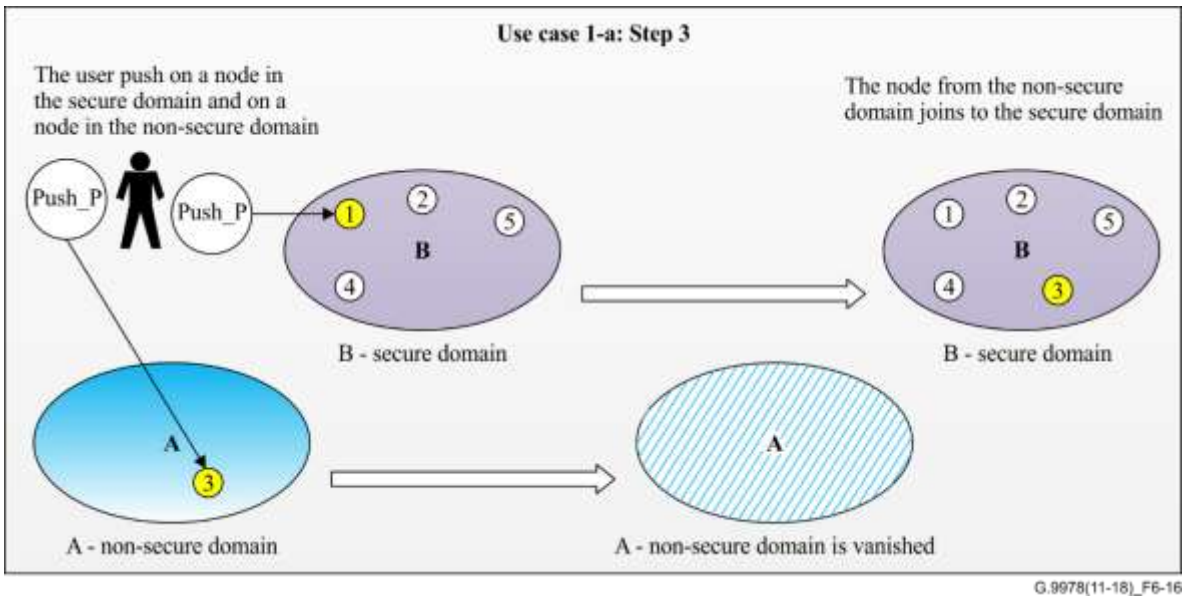

Figure 6-16 – Use case 1-a: Step 3 – The entire domain becomes secure domain

6.2.1.1.1 Use case 1-b – Add a node in unconnected state to a secure domain

This use case is a subcase of case 1-a. It refers to single-node pairing mode.

This use case describes a node that is configured to work only in an SD and therefore it is configured with an unconnected DN. Such a node, after power up, shall stay in an UNCONNECTED state, waiting for a PUSH_P event. During the time the node is waiting for the PUSH_P event, it shall not join any NSD and it shall not transmit any MAP frames.

6.2.1.2 Use case 2-a – Add a node from a non-secure domain to an existing secure domain

This use case refers to the single-node pairing mode and the multi-node pairing mode, where the user wants to add a new node to an SD. The secure domain already exists. The initial state of the joining node can be EP or DM.

The user has to send the PUSH_P event to a new node and the PUSH_P to one of the nodes of the SD. On pairing completion, the new node joins the SD. See Figure 6-17.

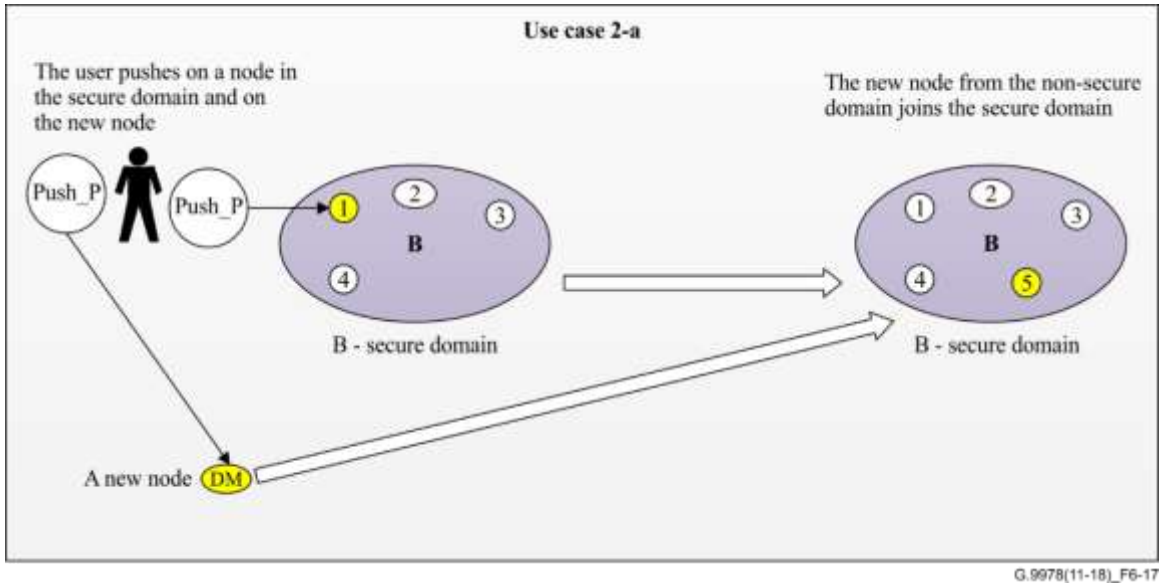

Figure 6-17 – Use case 2-a: A new node is added to a secure domain

6.2.1.2.1 Use case 2-b – Add a node that is in an unconnected state to an existing secure domain

This use case refers to single-node mode and multi-node pairing mode. It is subcase of case 2-a.

The use case describes an SD where the user wants to add a new node that is in an unconnected state. A node is in an unconnected state when it is configured with an unconnected domain name. The user has to trigger the PUSH_P event in the new node and in one of the nodes in the SD. On pairing completion, the new node is added to the SD. See Figure 6-18.

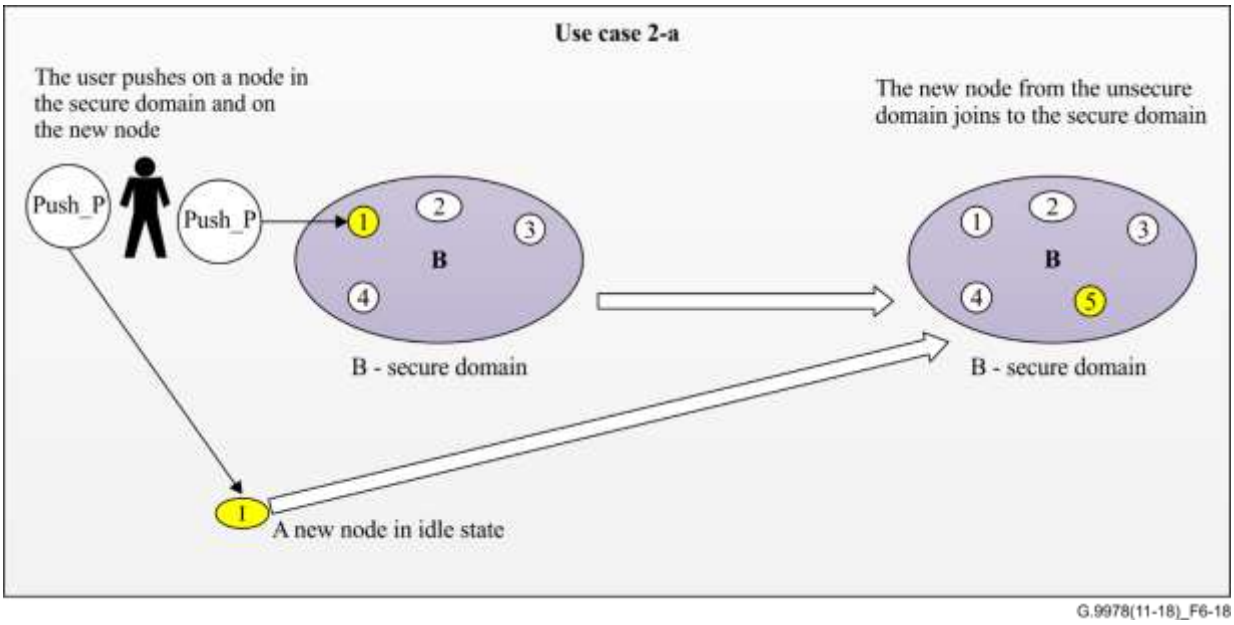

Figure 6-18 – Use case 2-b: A new node in an UNCONNECTED state is added to a secure domain

6.2.1.3 Use case 3 – A node that was already paired is switched on again

This use case refers to the single-node mode and to the multi-node pairing mode.

After power up, the powering-up node shall join the secure domain it was member of before power-down.

A node that is member of an SD (after successful pairing) that is turned off and then turned on again shall follow the default G.hn procedure for registration and authentication (clauses 8.6.1.1 and 9.2.2, Authentication to the domain of [ITU-T G.9961]).

6.2.1.4 Use case 4 – Power up of a node with an unconnected domain name

This use case is applicable to the single-node mode and to the multi-node pairing mode.

This case describes a node that is configured with an unconnected domain name. In this case, such a node is allowed to operate only within an SD. Such a node, after power up, shall stay in an UNCONNECTED state, waiting for a PUSH_P event. During the time that this node is waiting for the PUSH_P event, it shall not join any domain and it shall not become a DM.

6.2.1.5 Use case 5 – In multi-node pairing mode, convert a non-secure domain into a secure domain

This use case refers to the multi-node pairing mode. All nodes that detect the PUSH_P event will establish a secure domain.

In this use case, in order to convert an NSD to an SD, the user has to trigger the PUSH_P event in all nodes in the NSD within one pairing window.

One of the nodes becomes the DM of a new established secured domain and the other nodes join the SD as illustrated in Figure 6-19.

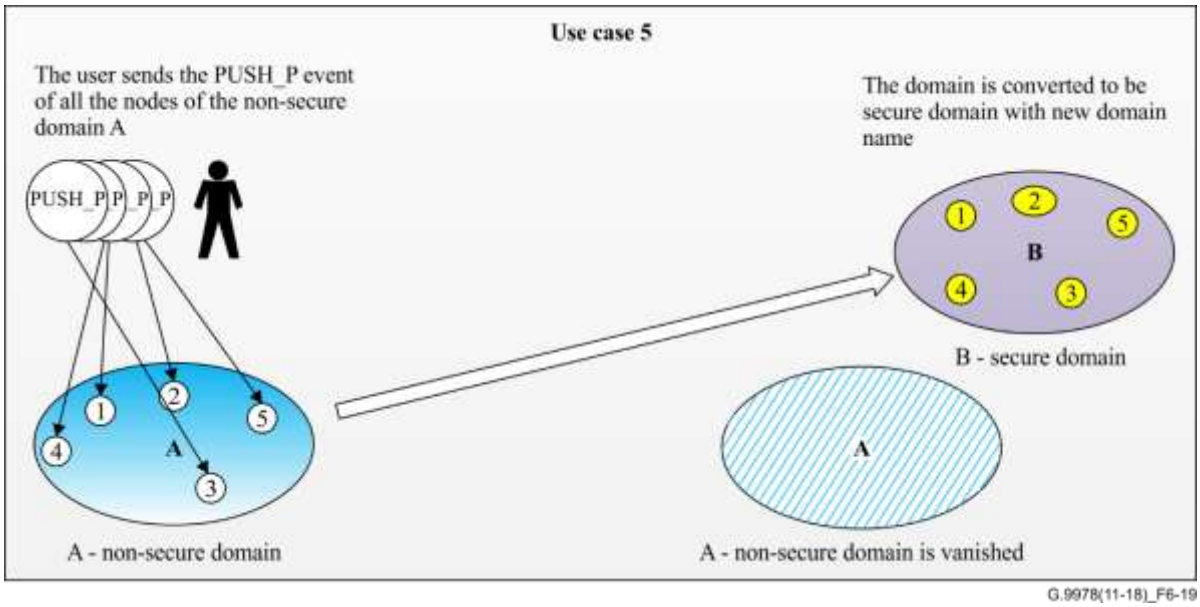

Figure 6-19 – Use case 5: In multi-node pairing mode convert a non-secure domain to a secure domain

6.2.1.6 Case 6 – Multi-node pairing mode: Add multiple nodes from a default domain or in an unconnected state

This use case refers to the multi-node pairing mode.

All the nodes from the non-secure domain or in unconnected state that detect the PUSH_P event shall join the secure domain.

A user triggers the PUSH_P event in a node of the SD and, within one pairing window, triggers the PUSH_P event in several nodes of an NSD or in an UNCONNECTED state. All the nodes from the NSD where a PUSH_P event was triggered shall join the SD. See Figure 6-20.

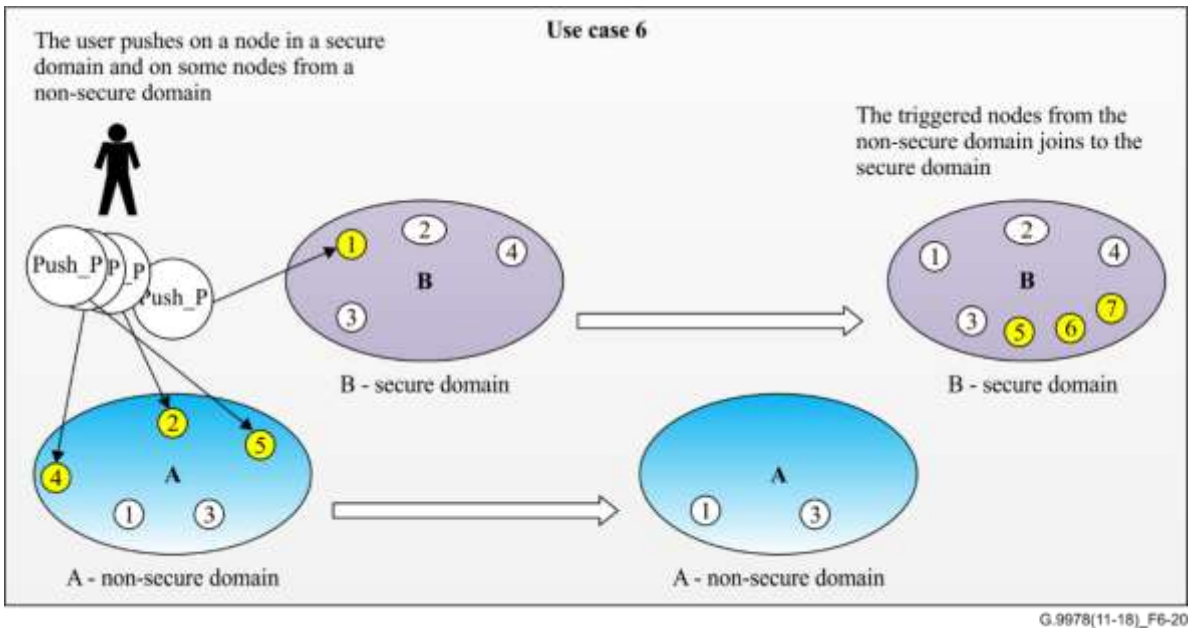

Figure 6-20 – Use case 6 – Multi-node generic pairing

6.2.1.7 Fault case 7-a – PUSH_P event on only one node of a non-secure domain

This fault case is applicable to the single-node mode and to the multi-node pairing mode. The node stays in a non-secure domain.

In this fault case, the user triggers the PUSH_P event on only one node of an NSD. In this fault case, nothing should happen.

This case is considered as a faulty case, because the user does not complete the pairing procedure. In this case, after the pairing window has expired, the node shall ignore the PUSH_P event and shall return to its previous state (i.e., the state it was before the PUSH_P event). See Figure 6-21.

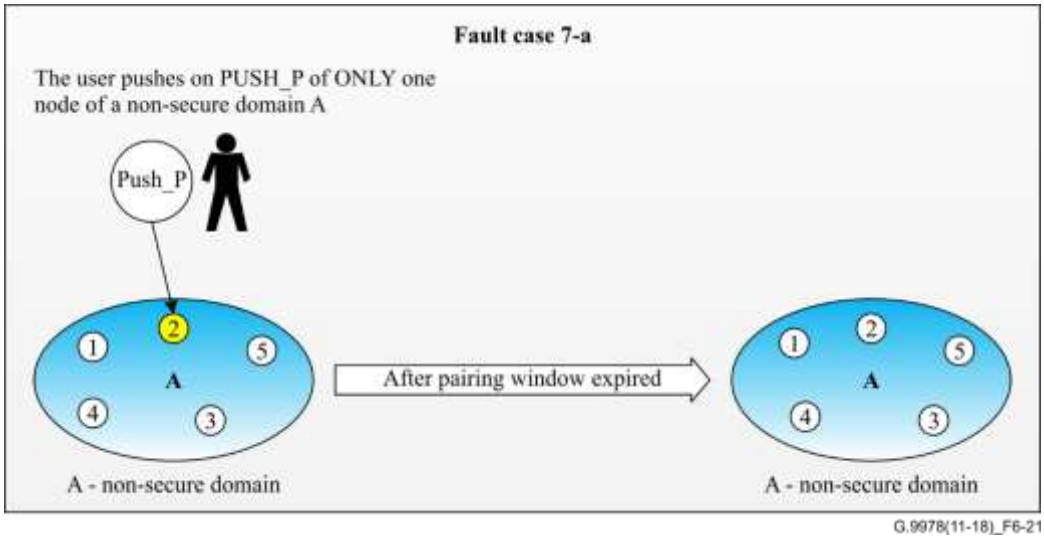

Figure 6-21 – Fault case 7-a

6.2.1.7.1 Fault case 7-b – PUSH_P event on only one node that is in an unconnected state

This fault case is a subcase of 5-a. It refers to a case where the user triggers the PUSH_P event on only one node that is in an unconnected state. After the pairing window duration, the node stays in an unconnected state.

In such a scenario nothing should happen.

This case is considered as a faulty case because the user does not complete the pairing procedure. In this case, the node shall ignore the PUSH_P event and return to its previous state before the PUSH_P event was triggered (i.e., as a node in an unconnected state waiting for a PUSH_P event). See Figure 6-22.

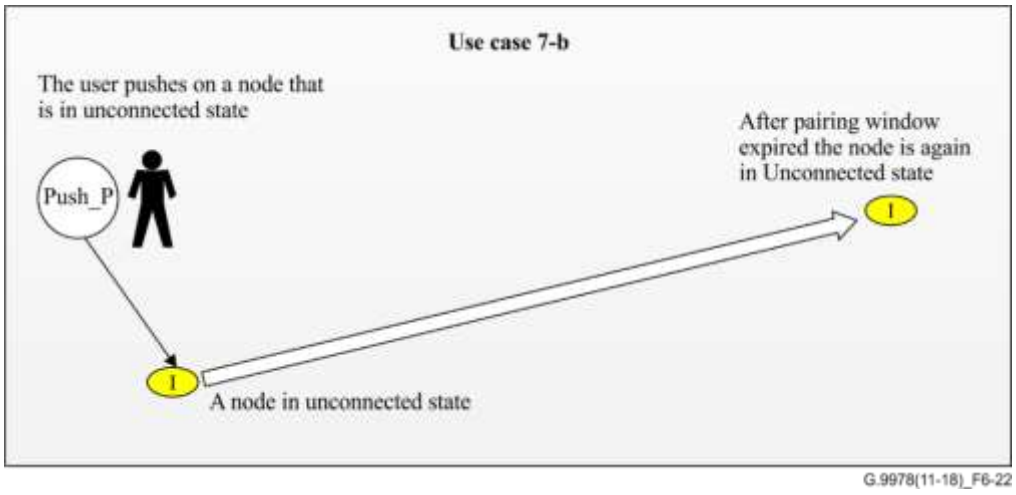

Figure 6-22 – Fault case 7-b

6.2.1.8 Fault case 8 – PUSH_P event on only one node in a secure domain

This use case refers to the single-node mode and to the multi-node pairing mode.

The node will open or ask the DM to open the pairing window, and then close it after the pairing window duration with no other action**.**

In this case, a PUSH_P event is triggered on only one node in an SD, without completing any pairing procedure. In this case, the triggered node shall inform its DM about the PUSH_P event without any change in the domain. See Figure 6-23.

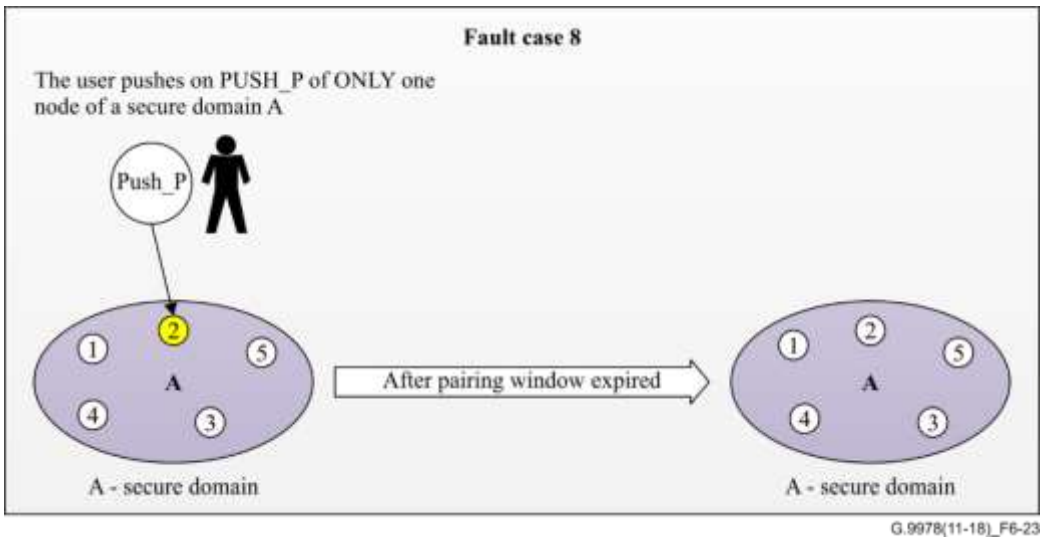

Figure 6-23 – Fault case 8

6.2.1.9 Fault case 9 – User tries to add two nodes within one pairing window

This use case refers only to the single-node pairing mode.

Only one of the nodes from the non-secure domain shall join the secure domain, and the other node shall not create its own secure domain and shall return to its previous state before the PUSH_P event.

In this case, the user triggers the PUSH_P event in two nodes that are in an NSD and in one node of an SD. The first node that successfully completed the pairing procedure shall join the SD. The second node shall be rejected by the SD and shall return to its previous state before the PUSH_P event. See Figure 6-24.

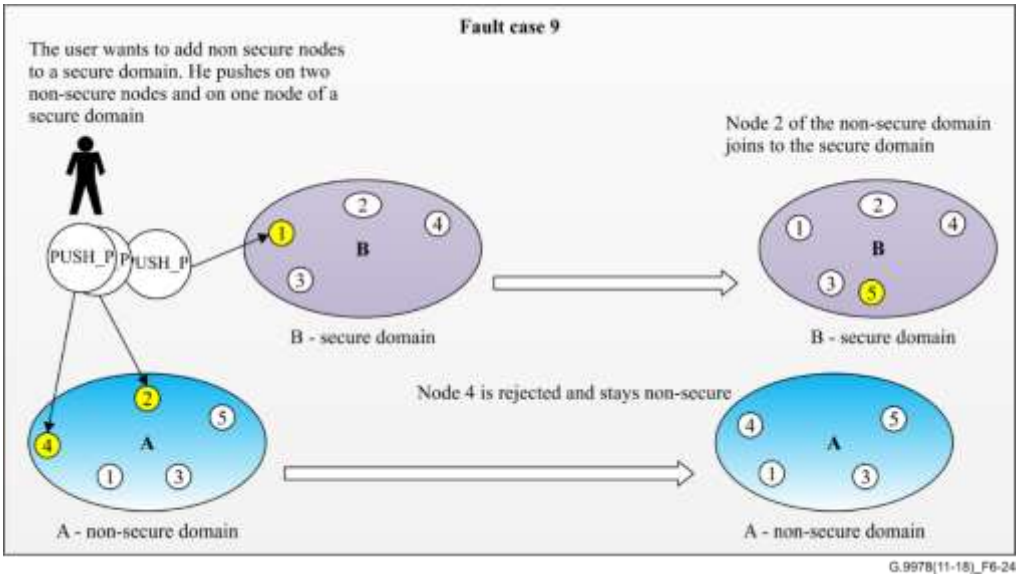

Figure 6-24 – Fault case 9

6.2.1.10 Use case 10 – User triggers PUSH_R event on a node in a secure domain

In this case, the user triggers the PUSH_R event on a node that is in an SD network.

After triggering the PUSH_R event, the node shall resign from the domain, and move into unconnected state.

When a node that belongs to an SD receives a PUSH_R event, it shall initiate a self-resignation procedure from its current domain and, without waiting for any confirmation from the DM, it shall move to IDLE state and set its DN and PW to the default values.

6.2.1.11 Use case 11 – Single node pairing by user confirmation

In this case, when a new node first powers on, it will broadcast a message to notify the network of its existence. When DM receives the message, it will trigger a Flash-E event, such as light flashing on the DM, asking whether the new node is allowed to join the secure domain. If the user chooses to agree to it, the user will push a button, and the new node will join the secure domain.

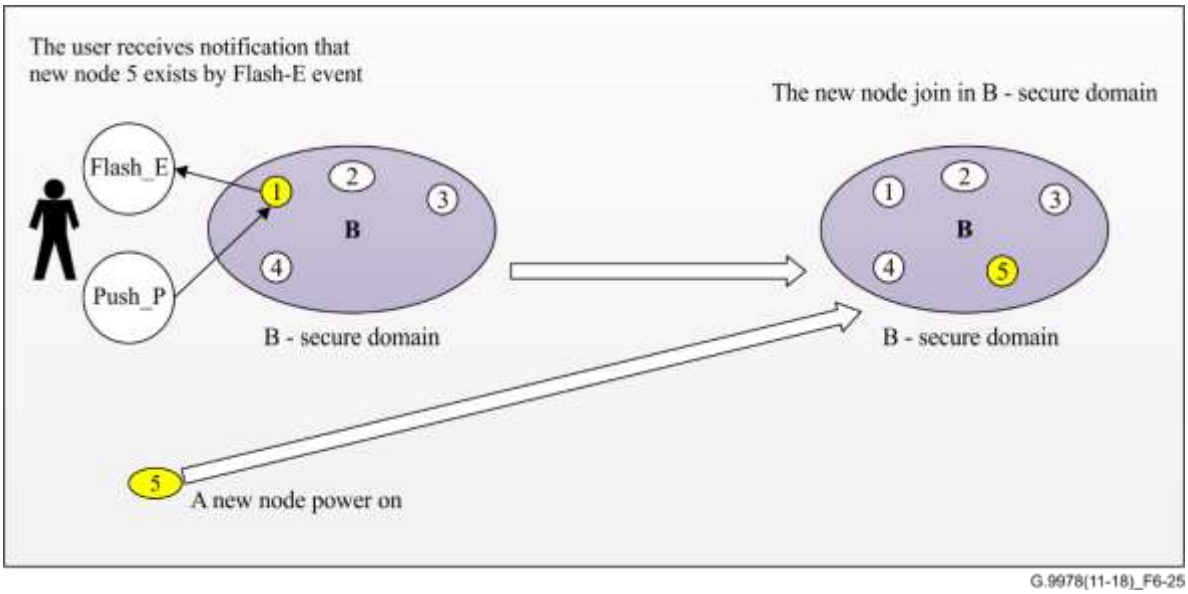

Figure 6-25 – Flash_E event to notify the existence of a new node. The user chooses whether allow it join in secure domain by PUSH_P event

NOTE – Nodes in the neighbourhood may also receive the notification message and trigger the Flash-E event. The vendor should implement vendor discretionary means to avoid security issues related to this.

6.2.2 Secure admission by generic pairing

A generic pairing mechanism enables the user to convert an NSD to an SD or to add one or more unconnected nodes to an SD by a simple push event operation, without the need for any computer communication with the nodes in the domain.

Both single-node pairing and multi-node pairing modes shall be supported. A domain shall operate in only one of these, according to its configuration. Single-node pairing is specified in clause 6.2.2.1 and multi-node pairing is specified in clause 6.2.2.2. See Table 6-10.

Table 6-10 – System parameters for the pairing mechanism

Parameter	Description	Medium			
		Power-line baseband	**Coax baseband (BB)**	**Coax radio frequency (RF)**	**Phone line**
$T_{PAIRING}$ (Note)	Pairing window that starts after a PUSH_P event. During this period, the DM shall confirm the registration pairing request	60-300 s	60-300 s	60-300 s	60-300 s
T_EP_INTERVAL	The interval that a joining node is acting as an EP trying to pair with a secure domain until it shall alternate with a temporary domain master	1 s	1 s	1 s	1 s
T_TMPDM_ INTERVAL	Period of time that a joining node during a pairing procedure shall act as temporary domain master before it alternates with an EP node for scanning	Random value in the range 4-8 s	Random value in the range 4-8 s	Random value in the range 4-8 s	Random value in the range 4-8 s
NOTE – The value of $t_{PAIRING}$ is vendor discretionary and is usually fixed by an external entity (e.g., HomeGrid Forum, [b-HomeGrid]).					

6.2.2.1 Single-node pairing procedure description

The single-node pairing procedure is used to convert an NSD to an SD or to add an unconnected node or a node from an NSD to an SD. In order to convert an NSD to an SD, the user should trigger the PUSH_P event in two nodes of the NSD within the $t_{PAIRING}$ time period. During the pairing procedure, one of the two pairing nodes should become the DM of the new established SD and the other should register with this DM and become a member of this new established SD.

In order to add a node that is not in an SD to an existing SD, the user should trigger the PUSH_P event in the non-secure node and in one of the nodes of the SD.

A node that is not in an SD that detects a PUSH_P event cannot know in advance if it should register in an existing SD or if it should establish a new SD. Therefore, on detection of the PUSH_P event, it should try to pair with any detected SD for $t_{PAIRING}$ time. After this time expires, it shall establish an SD, but it shall also temporally monitor the network transmissions looking for already established SDs until successful completion of the pairing procedure or expiry of $t_{PAIRING}$. During this period, the DM acts therefore as a "temporary DM".

In order to establish an SD, the node shall create a random SDN and it shall transmit MAPs to enable any potential node to pair with it. In parallel with acting as a temporary DM, the node shall scan for MAPs of other SDs and may decide to register in another domain as an EP node.

If the node tries only to register in an SD and it is actually the case where the user wishes to establish an SD, both triggered nodes would scan for MAPs of an SD without having any DM transmitting MAPs of an SD and able to accept their registration request. For this reason, only one of the triggered nodes should become a DM.

The temporary DM behaviour can be implemented either by making use of the t_2 timing described in clause 8.6.6.1.1 of [ITU-T G.9961] or by implementing a mechanism to alternate between the DM and EP states described in clause 6.2.2.1.1.1.

6.2.2.1.1 Alternating between domain master and endpoint states

Due to the fact that there is no arbitrary way to define which of the two triggered nodes shall be the DM of the new SD, each node should alternate on detection of a PUSH_P event between:

– acting as a temporary DM to enable the other node to pair with it;

– registering in any detected SD.

This behaviour should last until successful completion of the pairing procedure or expiry of $t_{PAIRING}$.

The temporary DM shall act alternately as a temporary DM for several seconds and as a registering node for another period of time. In order to ensure that during the time that one of the pairing nodes is acting as a temporary DM the other node is in the phase of scanning for an SD, the following timing scheme shall be used.

The period of time that the pairing node is acting as a temporary domain shall be longer than the period of time that it is acting as an EP node in the scanning phase. The period of time that a node shall act as a temporary DM shall be randomly selected within the range from 1 s to 4 s while the time that a node shall be in a scanning state as registering EP node shall be fixed at 1 s. This way, the scanning node will always detect the second pairing node in its temporary DM state as illustrated in following time schema. The pairing opportunity arrows in Figure 6-26 illustrate the opportunity that each registering node has to detect the temporary DM.

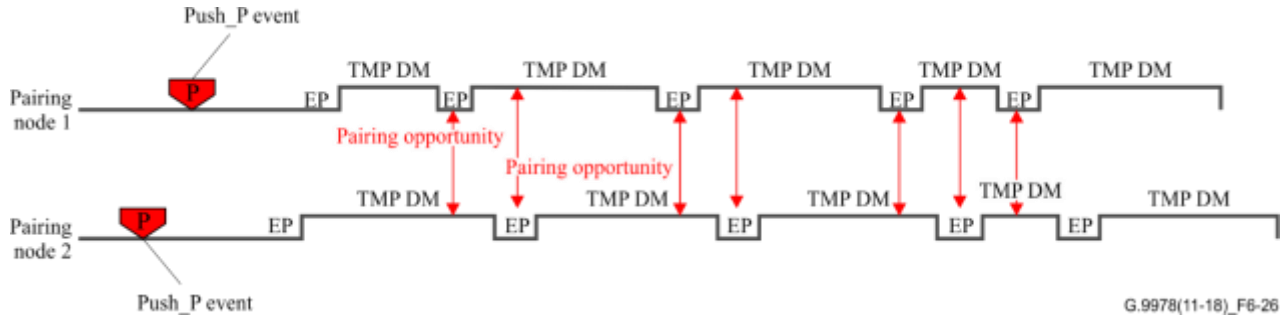

Figure 6-26 – Timing scheme for temporary domain master and endpoint state alternation

Figure 6-27 illustrates a pairing between node 2 and node 1 that was successfully completed when node-2 was acting as a temporary DM and node-1 was acting as an EP. After the pairing is successfully completed, both nodes stop alternating and the temporary DM continues as a temporal DM while the EP continues as an EP node.

Scenario of success pairing between node 1 as EP and node 2 as TMP DM.
After successful registration node 2 continue to be TMPDM and node 1 continue as EP

Figure 6-27 – Timing scheme for temporary domain master and endpoint state alternation

6.2.2.1.2 Example in a state machine of a PUSH_P event in single-node pairing mode

Figure 6-28 illustrates the state machine of a node that is in unconnected mode or a member of an NSD after a PUSH_P event is triggered in single-node pairing mode.

The procedure in this example makes use of the alternation between DM and EP states described in clause 6.2.2.1.1.

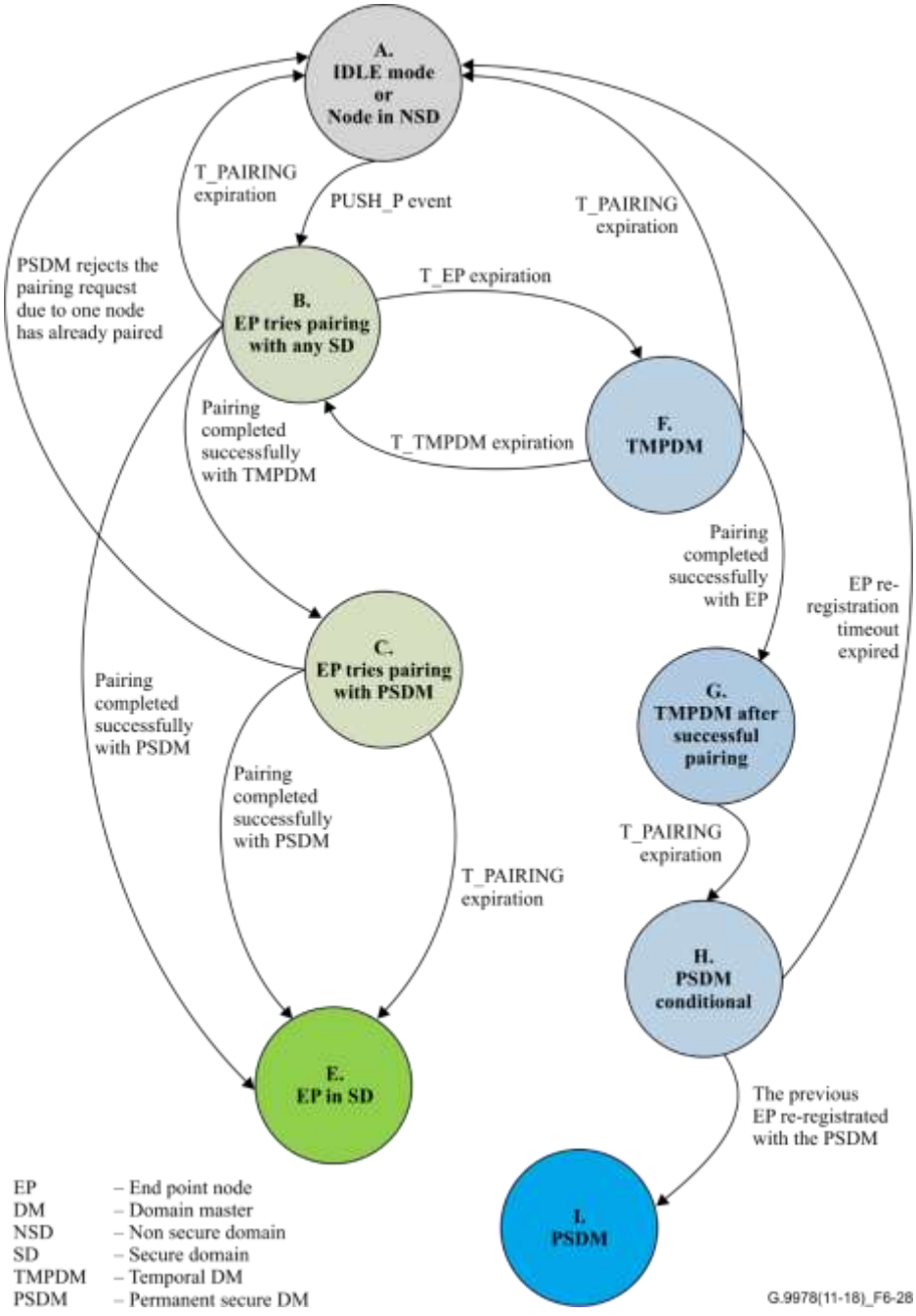

Figure 6-28 – State machine for a node triggered by a PUSH_P event in the single-node pairing mode

The following list describes each state of the state machine illustrated in Figure 6-28 and the events that make the node transitions from one state to the next according to the event.

A. **Unconnected mode or node in an NSD** – This state is that for a node that is in an unconnected state or for a node that is in an NSD. After a PUSH_P event, the node changes to state B.

B. **EP tries pairing with any SD** – In this state, the EP node scans for any SD for a T_EP interval (1 s). If it detects a secure DM, it shall try to pair with the DM of the SD. One of four events can make the node leave this state.

1) **T_EP expiry** – The T_EP interval has expired. On this event, the EP stops acting as an EP and starts acting as a temporary DM in the state: **F. (TMPDM**).
2) **Pairing successfully completed with a TMPDM (temporal domain master)** – The EP node successfully completed a pairing procedure with a temporary DM. This event transitions the EP to state C. [EP tries pairing only with a permanent secure domain master (PSDM)].
3) **Pairing successfully completed with a PSDM** – The EP successfully completed a pairing procedure with a PSDM). This event transitions the EP to the final state: EP in an SD.
4) **T_PAIRING expiry** – the timer that counts the pairing windows has expired. This event transitions the EP to state A where it was before the PUSH_P event. This means that the pairing procedure is ended without any successful pairing.

Figure 6-29 illustrates the algorithm of the EP in state B.

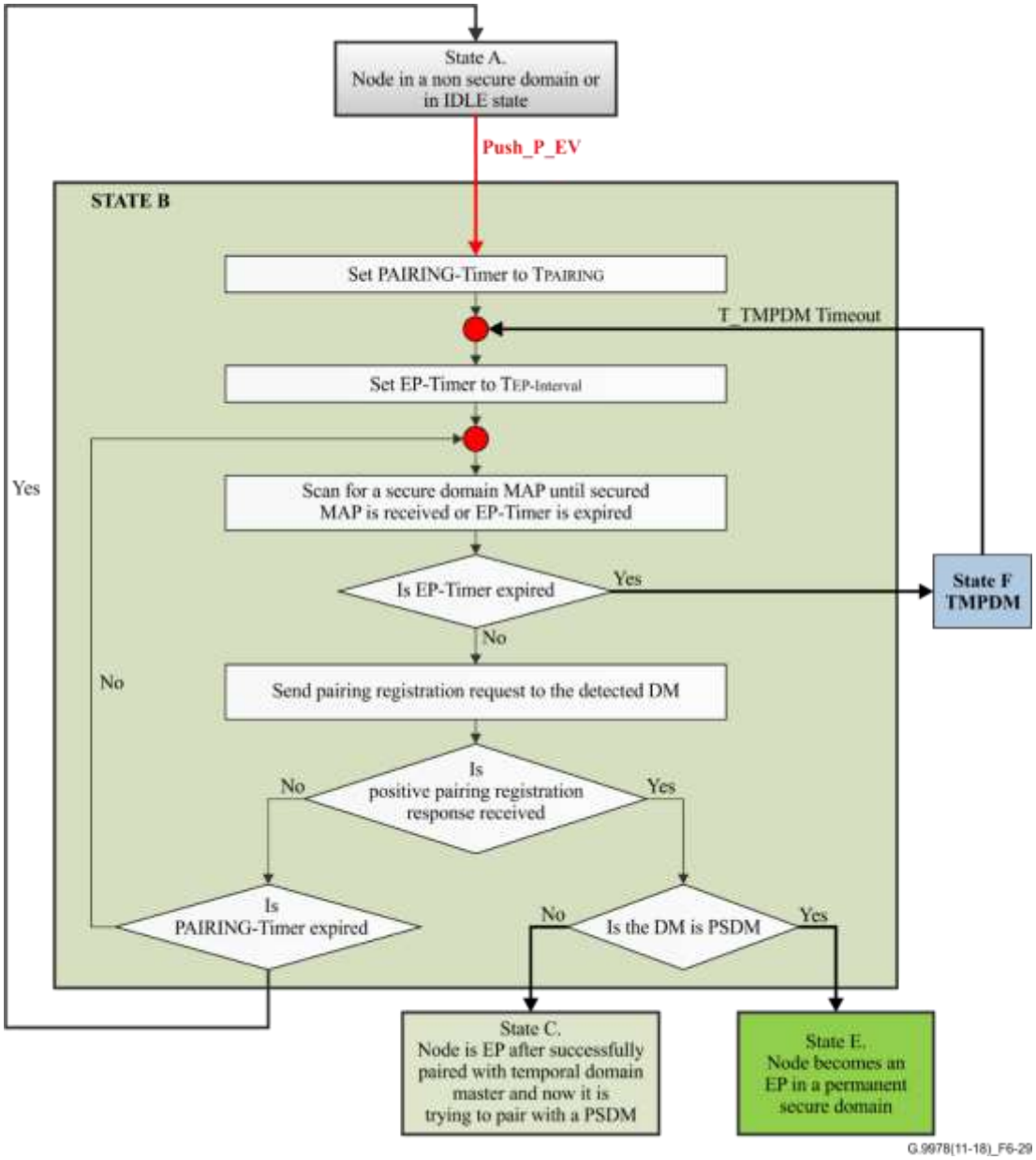

Figure 6-29 – Algorithm for state B: Endpoint tries pairing with any secure domain

C. **EP tries pairing only with a PSDM** – In this state, the EP is already paired with the temporary DM and acts as a normal registered node, including the execution of the authentication procedure specified in [ITU-T G.9961]. During this state, the EP shall continue to try to pair with any other detected PSDM in order to avoid fault case 9, when the user wants to add a node to an SD, but it pushes buttons on two nodes that are not in the SD and on one node from the SD. In such a case, the node shall return to state A. On one of the following four events, the node may transition from this state to another state.

1) **Pairing successfully completed with a PSDM** – The EP node successfully completed a pairing procedure with a PSDM. This event transitions the EP to final state E. The EP is in an SD.
2) **T_PAIRING expiry** – The timer that counts the pairing windows has expired. This event transits the EP to intermediate state D. The EP tries to re-register with a TMPDM.
3) **The PSDM rejected the pairing due to one node already being paired** – The responding PSDM rejects the pairing request because it had just closed its pairing window since it had successfully completed the pairing procedure with another node. (A PSDM shall send this rejection when it receives a pairing request within the last T_PAIRING but had already paired successfully with another node.)

Figure 6-30 illustrates the algorithm of the EP in state C.

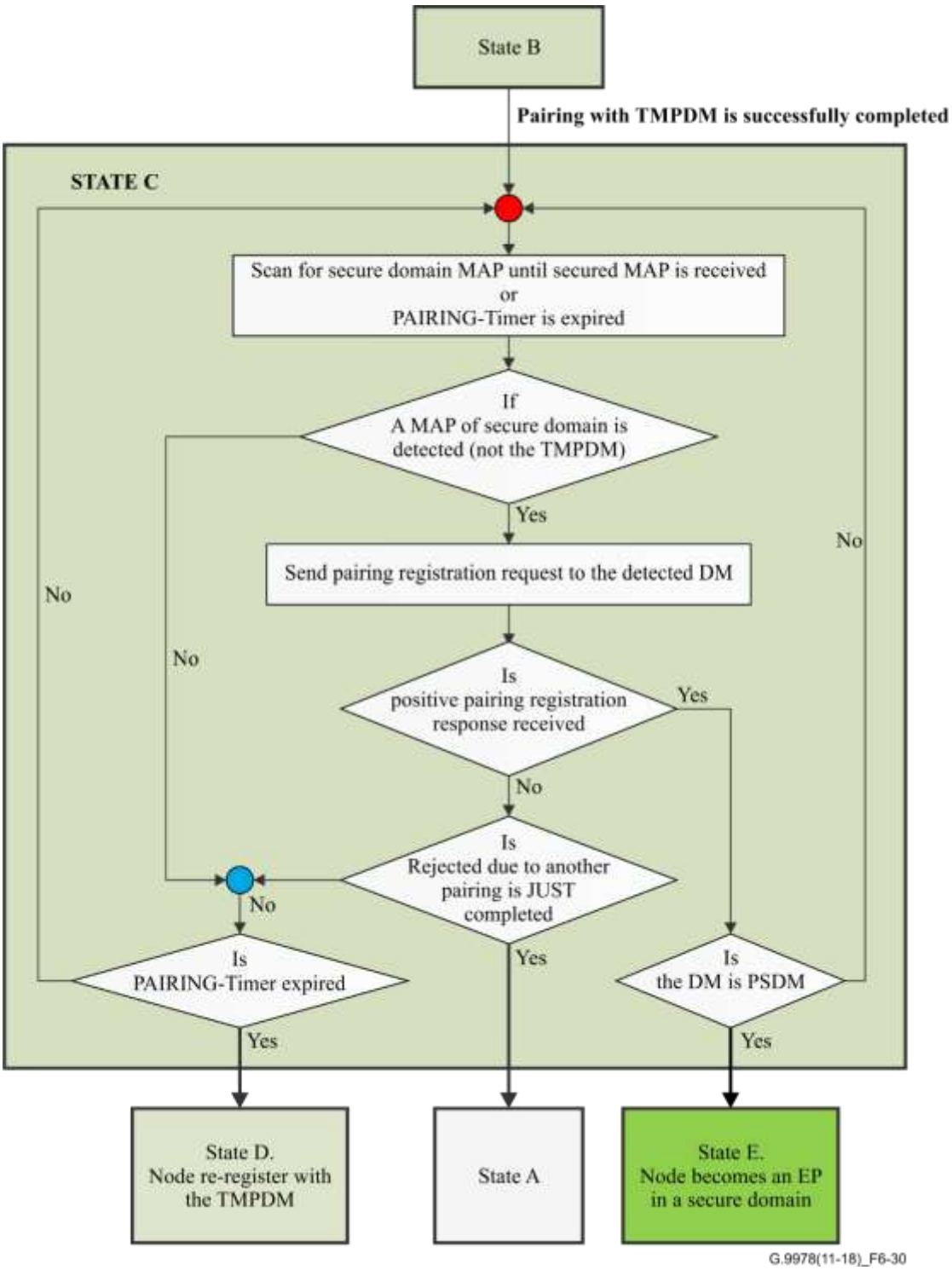

Figure 6-30 – Algorithm for state C: EP tries pairing only with a permanent secure domain master

D. **EP re-registers with a TMPDM** – In this state, the EP node shall try to re-register with its original TMPDM that it had already paired with in event B 2). There are two events that trigger a transition from this state, as follows.

1) **The EP re-registers successfully with its TMPDM** – This event shall trigger a transition of the EP to final state **E**.

2) **The EP fails to re-register with its TMPDM** – The EP retries to re-register with its TMPDM expired (the TMPDM is off). This event shall abort the pairing procedure and transition the EP to final state **A**.

See Figure 6-31.

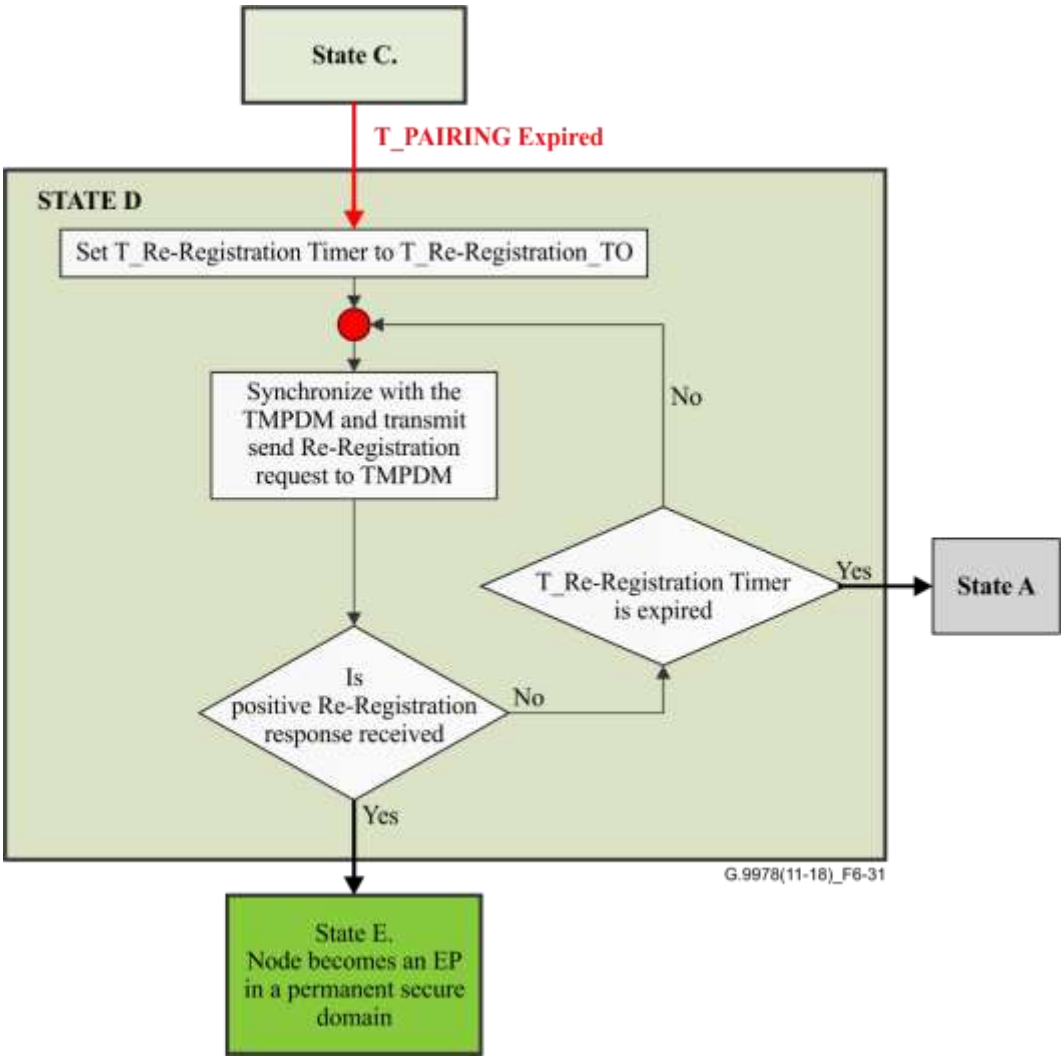

Figure 6-31 – Algorithm for state D: Endpoint re-registers with a temporal domain master

E. **EP in SD** – This is a final state for the node. In this state, the node has finally completed the pairing procedure and has become a member of an SD. In this state, the node starts the authentication procedure.

F. **TMPDM** – In this state the EP starts acting as a temporary DM for a period of time of a TMP_Interval. The first time that the EP transits to this state it shall generate a random DN and a PW. One of the following four events make the node transition from this state.

1) **T_TMPDM expiry** – The timer that counts the interval that the node shall act as a temporary DM has expired. On this event, the temporary DM shall stop acting as a temporary DM and switch to act as an EP node in state B. (EP tries pairing with any SD.)

2) **Pairing successfully completed with an EP** – An EP node has successfully completed the pairing procedure with this temporary DM. This event makes the temporary DM transition to state G. TMPDM after successful pairing.

3) **T_PAIRING expiry** – The timer that counts the pairing windows has expired. This event shall abort the pairing procedure and make the node transition to state A where it was before the PUSH_P event (unconnected mode or a node in an NSD).

Figure 6-32 illustrates the algorithm of the TMPDM in state F.

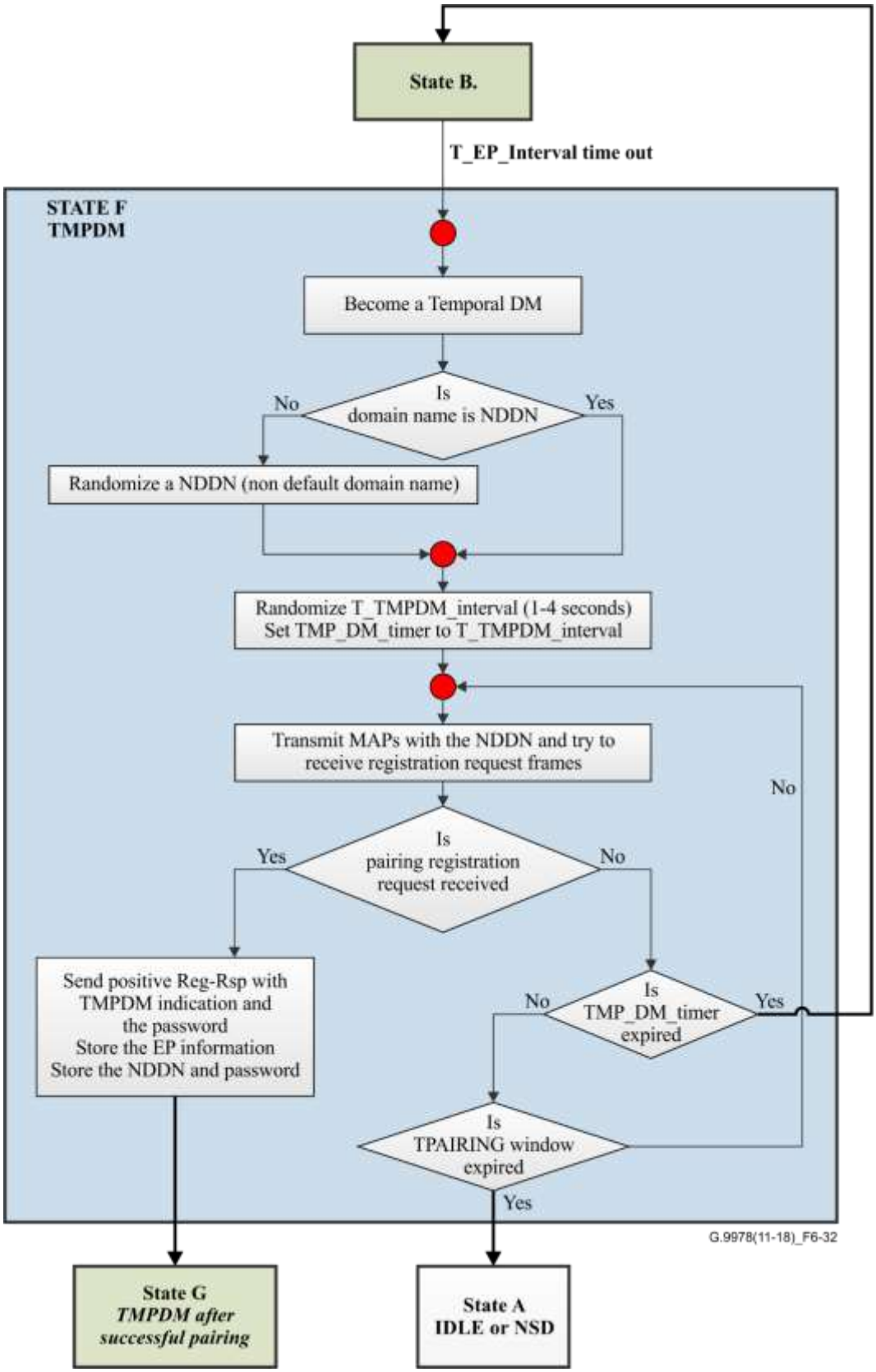

Figure 6-32 – Algorithm for state F. TMPDM

G. **TMPDM after successful pairing** – In this state, the temporary DM continues to act as a temporary DM until T_PAIRING expiry. The temporary DM shall allocate a dedicated transmission opportunity (TXOP) for the registered EP for scanning and pairing with other potential DMs. The following events shall make the node transition from this state.

1) **Re-registration event** – The EP successfully completed the re-registration procedure. The EP completed its pairing procedure and therefore the temporary DM shall be converted to a PSDM.

2) **T_PAIRING expiry** – The timer that counts whether the pairing window has expired. This event makes the TMPDM transition to the intermediate state **H. PSDM conditional**.

H. **PSDM conditional** – This is an intermediate state in which the temporary DM becomes a conditioned PSDM, because it depends whether the EP that paired with it successfully in state F is still relevant and this EP did not pair meanwhile with another PSDM. In this state, the DM shall use the DN that it previously generated in state F. (TMPDM). The DM shall set a timer T_Re_Register that counts the timeout until the EP re-register with the DM. The timeout shall be specified according to the time of the pairing procedure that was executed in state F as determined by the formula:

timeout = T_PAIRING − (Pairing_t − Start_window_t) + 1 s

Pairing_t is the time when the pairing procedure with the EP is started. Start_window_t is the time when the node was triggered by a PUSH_P event. The following events shall transition the node from this state.

1) **The EP re-registered with the PSDM** – The EP that paired previously with the DM while it was in state F has re-registered with the DM. This event indicates to the DM that the EP has successfully completed a pairing procedure with it. Therefore the conditioned PSDM can be a PSDM. This event transitions the node to a final state **I. PSDM**.

2) **EP re-registration timeout expired** – This event occurs when the timer for re-registration of the EP with the conditional PSDM has expired. This can happen, for example, if the EP is successfully paired with the actual PSDM.

See Figure 6-33.

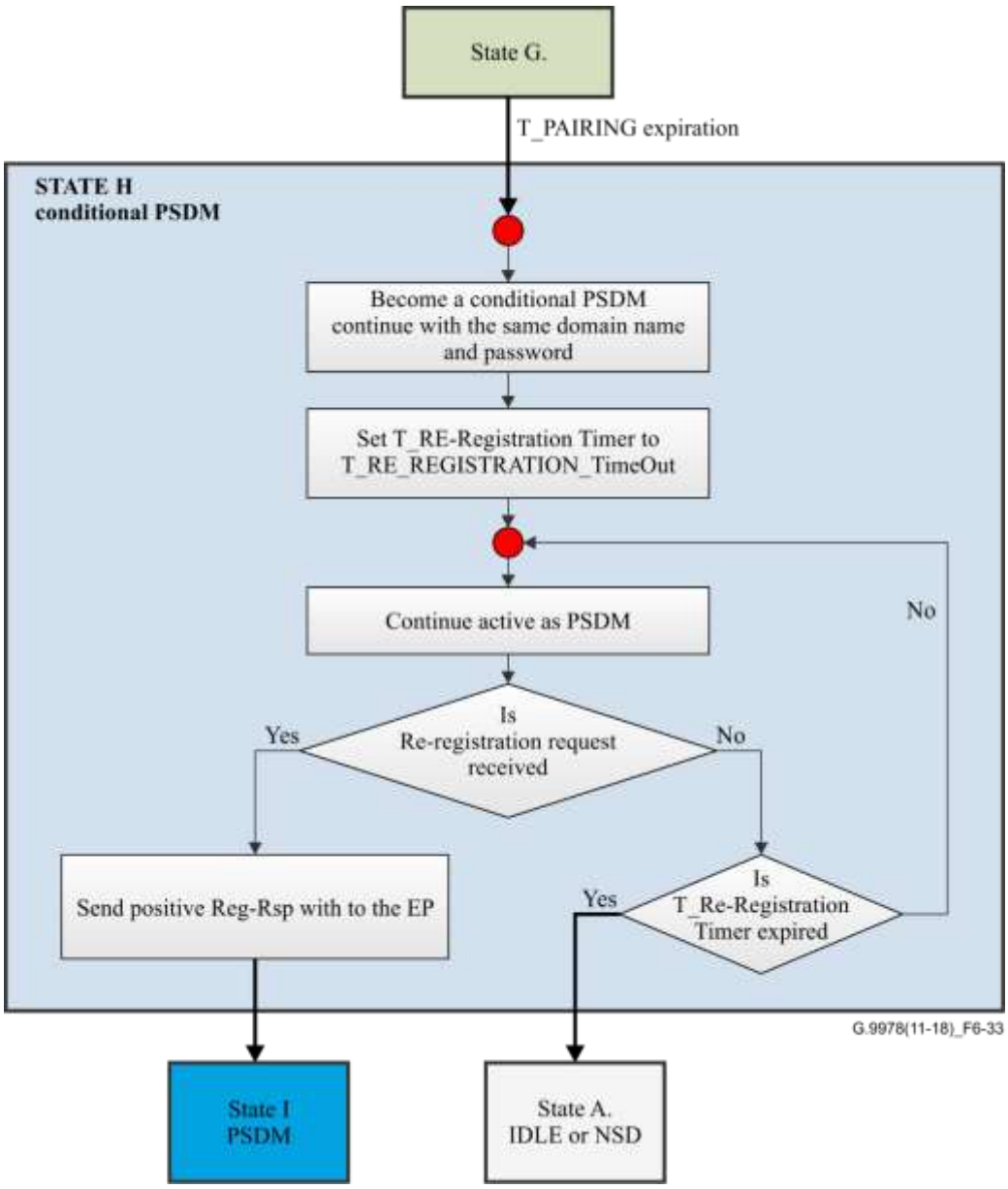

Figure 6-33 – Algorithm for a state H conditional permanent secure domain master

I. **PSDM** – This is a final state where the conditional secure DM becomes a PSDM after it receives a re-registration request from its EP. In this state, the PSDM shall use the DN and PW that it used in state F and in state H.

A node that starts a generic pairing procedure shall complete the pairing procedure in one of the following possible states.

– The node successfully joins an SD as an EP node (state E).

– The node working as a temporary DM becomes a permanent secure DM (state I).

– After expiry of the pairing window period without any successful completion of the pairing procedure, the triggered node returns to the state it was before the PUSH_P event (state A).

A PSDM shall operate after a PUSH_P event as specified in the algorithm depicted in Figure 6-34.

After a PUSH_P event, the PSDM shall enter into a pairing state. It shall exit from the pairing state on successful completion of a pairing procedure or expiry of the T_PAIRING timer. If the PSDM exits the pairing state after successful completion of a pairing procedure before T_PAIRING has expired and it receives other pairing requests from another node, it shall answer with a rejection response due to another pairing procedure having completed already.

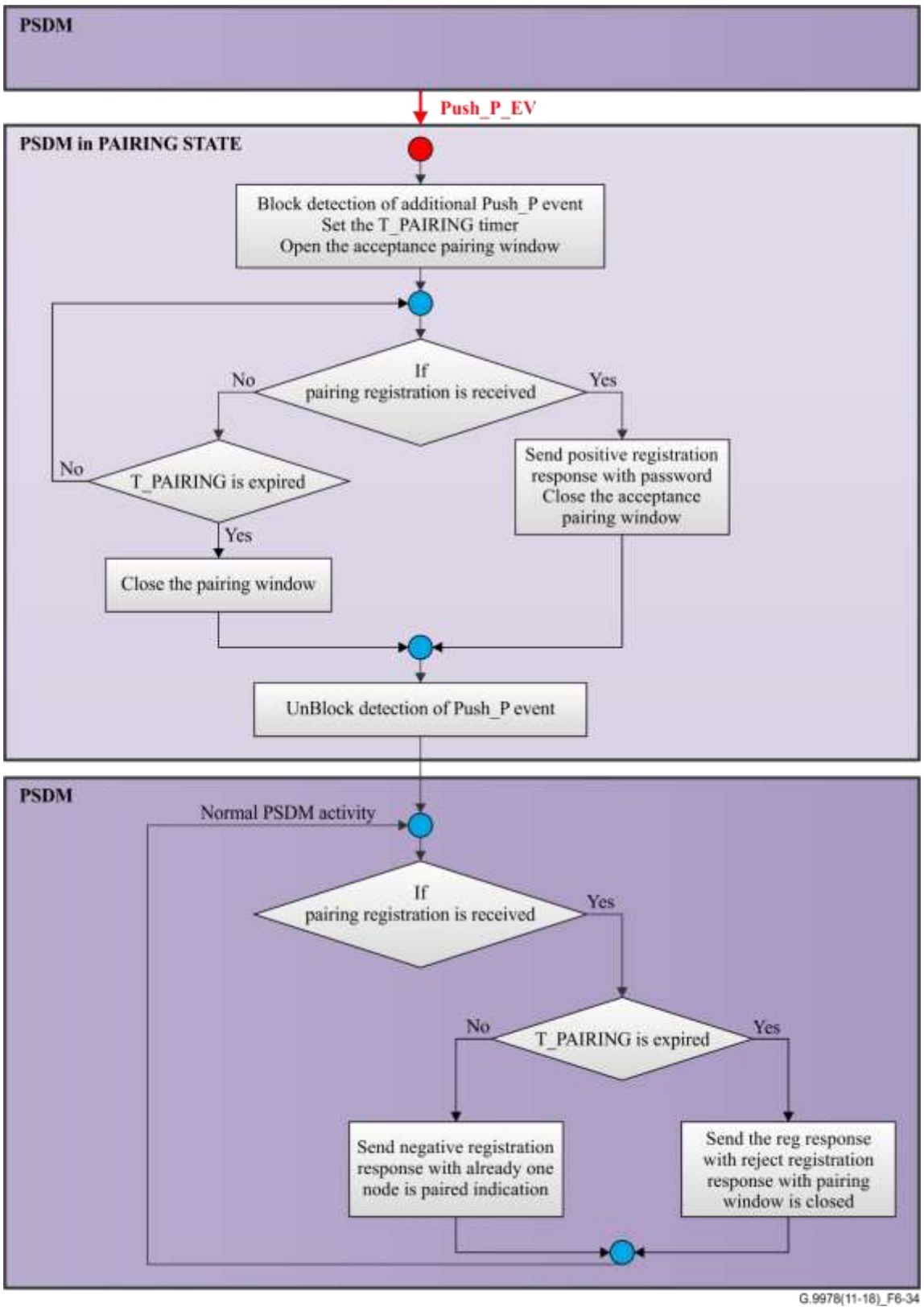

Figure 6-34 – Algorithm for a permanent secure domain master after a PUSH_P event

Figure 6-35 illustrates an example of faulty usage of the pairing mechanism by a user that triggered the PUSH_P event on four nodes that were in an unconnected state and on the DM of an SD. In single-node mode, the required result is that only one node shall join the SD and the rest of the triggered nodes return to the unconnected state. The pairing mechanism described in the foregoing

solves this faulty use case by having one node that joins the SD and the rest of the nodes return to the unconnected state.

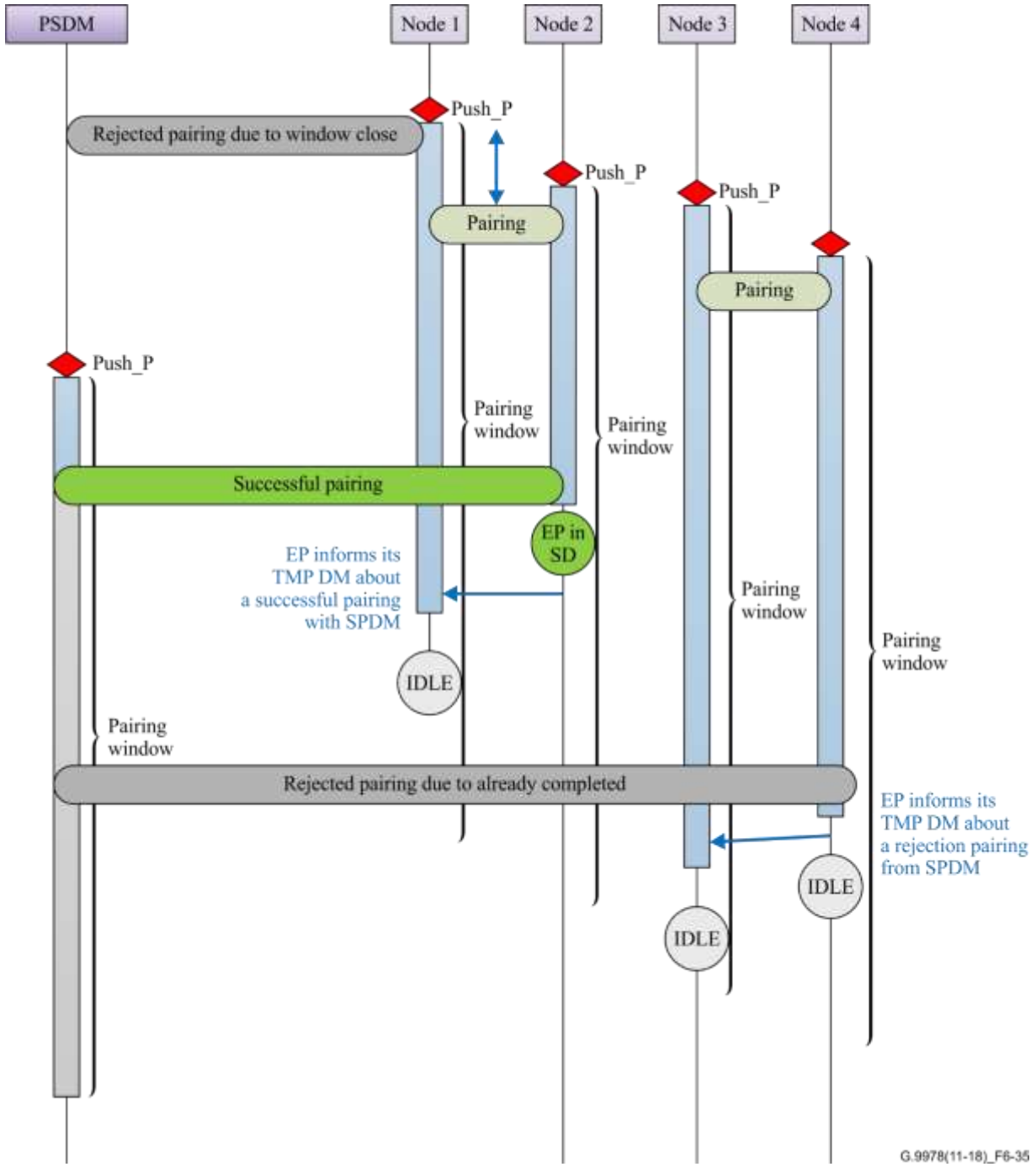

Figure 6-35 – Algorithm for a state H conditional permanent secure domain master

In this scenario, node 2 pairs with node 1 that is acting as a TMPDM. Then, node 3 pairs with node 4 that is acting as a TMPDM. Later, when node 2 successfully pairs with the PSDM, node 2 informs its temporary DM that it has registered successfully with a PSDM. The temporary DM, on receipt of this message, shall return to the UNCONNECTED state. Later, node 4 that tries to pair with the PSDM is rejected due to pairing being already successfully completed with another node (node 2). On receipt of this rejection from the PSDM, node 4 informs its temporary DM that it was rejected by a PSDM for the following reason "Pairing registration rejected due to pairing being already completed with another node" and returns to the unconnected mode. The temporary DM on receipt of this message also returns to the UNCONNECTED state.

6.2.2.1.3 Pairing registration protocol in the single-node pairing mode

The protocol of the pairing registration enables a node to register with an SD during the pairing procedure. The pairing registration protocol diagram is presented in Figure 6-36.

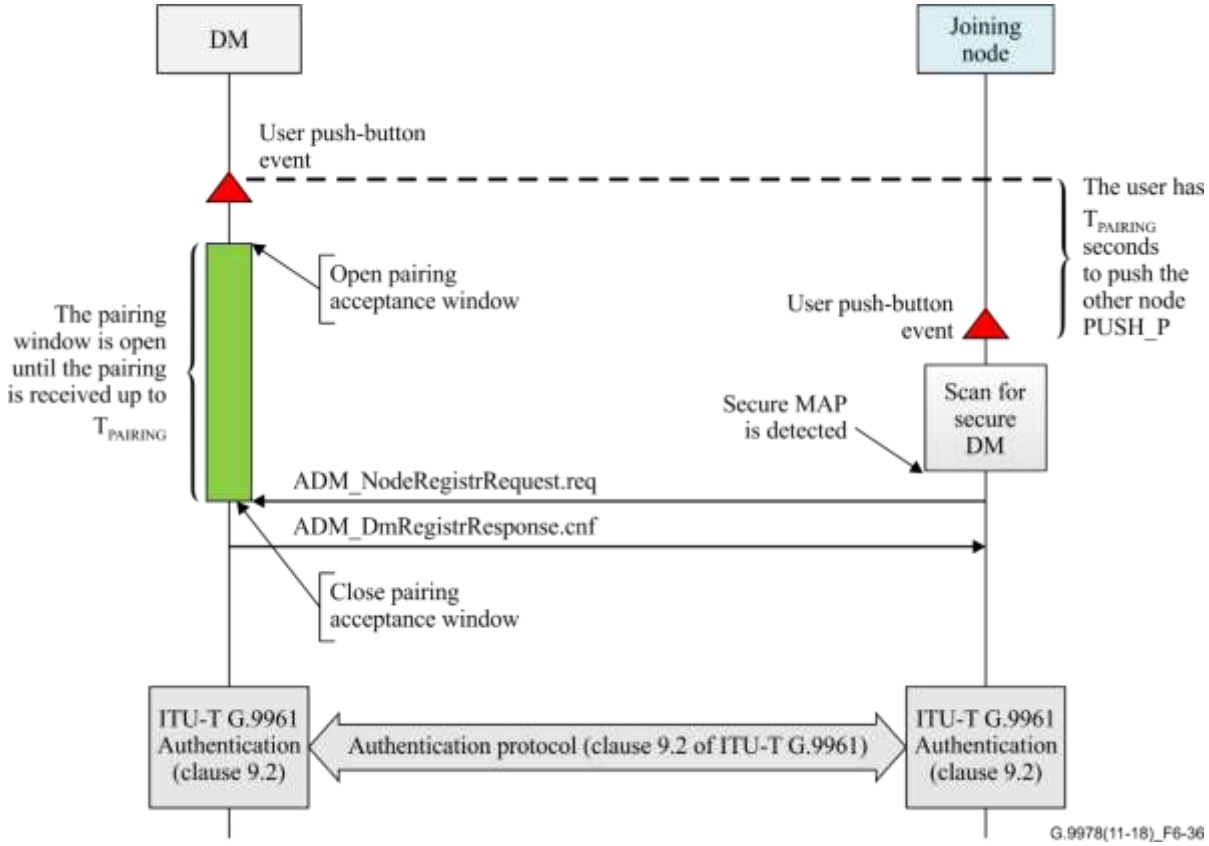

Figure 6-36 – Pairing registration protocol diagram in the single-node pairing mode

A node that is not a member of an SD that is triggered by a PUSH_P event shall try to register only with an SD, by sending an ADM_NodeRegistrRequest.req message to a detected secure DM. The ADM_NodeRegistrRequest.req message shall include the PairingReq field, in addition to all the parameters that are specified in clause 8.6.1.1.1 of [ITU-T G.9961].

NOTE – The security status of the domain is indicated in the security-related domain info subfield (see Table 8-85.9 of [ITU-T G.9961]).

On receipt of the ADM_NodeRegistrRequest.req message, the DM shall process the registration request and shall reply within REG_RESP_TIME to the node with an ADM_DmRegistrResponse.cnf message.

If the DM receives the registration request message while it was within a pairing window, the ADM_DmRegistrResponse.cnf message shall include the following fields:

– a status flag with a success registration indication;
– a PW needed for the authentication procedure (clause 9.2 of [ITU-T G.9961]);
– a non-zero DEVICE_ID for the registering node assigned by the DM;
– all other relevant configuration data as specified in [ITU-T G.9961].

On receipt of the ADM_DmRegistrResponse.cnf message, the registering node shall identify the ADM_DmRegistrResponse.cnf message based on its REGID field and adopt the DN of the domain that replied positively and its new assigned DEVICE_ID. The registering node shall use the PW included in the ADM_DmRegistrResponse.cnf message for the authentication procedure as specified in clause 9.2 of [ITU-T G.9961].

If the registration request is not received within an open pairing window, the secure DM shall reject the registration request by replying to the registering node with an ADM_DmRegistrResponse.cnf message that contains the status flag set to zero and an extended rejection code 3_{16} that indicates that the registration request is rejected for the reason that the "pairing window is closed" as specified in Table 8-15.1 of [ITU-T G.9961].

If the registration request is received within an open pairing window, but after another successful pairing, then the DM shall reject the registration request by replying to the registering node with a ADM_DmRegistrResponse.cnf message that contains the status flag set to zero and an extended rejection code 4_{16} that indicates that the registration request is rejected for the reason that "pairing has just been successfully completed with another node" as specified in Table 8-15.1 [ITU-T G.9961]. This code shall be sent up to 5 s after the window has been closed if the DM needs to reject a pairing request. After this time, the code used to reject a pairing request because the window is closed shall revert to 3_{16}.

In the case of rejection, the DEVICE_ID shall be set to zero.

The ADM_DmRegistrResponse.cnf message shall include all the other fields as specified in clause 8.6.1.1.1 of [ITU-T G.9961] and shall be sent as specified in clause 8.6.1.1.1 of [ITU-T G.9961] [medium access (MA) priority associated with medium access control protocol data unit (MPDU) priority = 7].

If the registering node does not receive an ADM_DmRegistrResponse.cnf message from the DM within 1 s, the node shall retry registration within REG_RETRY_TIMEOUT. If the joining node does not receive a response after MAX_REG_ATTEMPTS registration attempts, the node shall scan and try to detect another DM.

If the joining node was rejected by the secure DM, due to a closed pairing window, the node shall scan and try to detect another secure DM. The node shall continue to retry registration with all detected secure DMs during $t_{PAIRING}$. If the node does not receive a positive registration response after the $t_{PAIRING}$ period has expired, it shall return to its state before the PUSH_P event was detected.

Figure 6-37 shows the operation of a DM in an SD on receipt of the PUSH_P event in a single-node pairing mode.

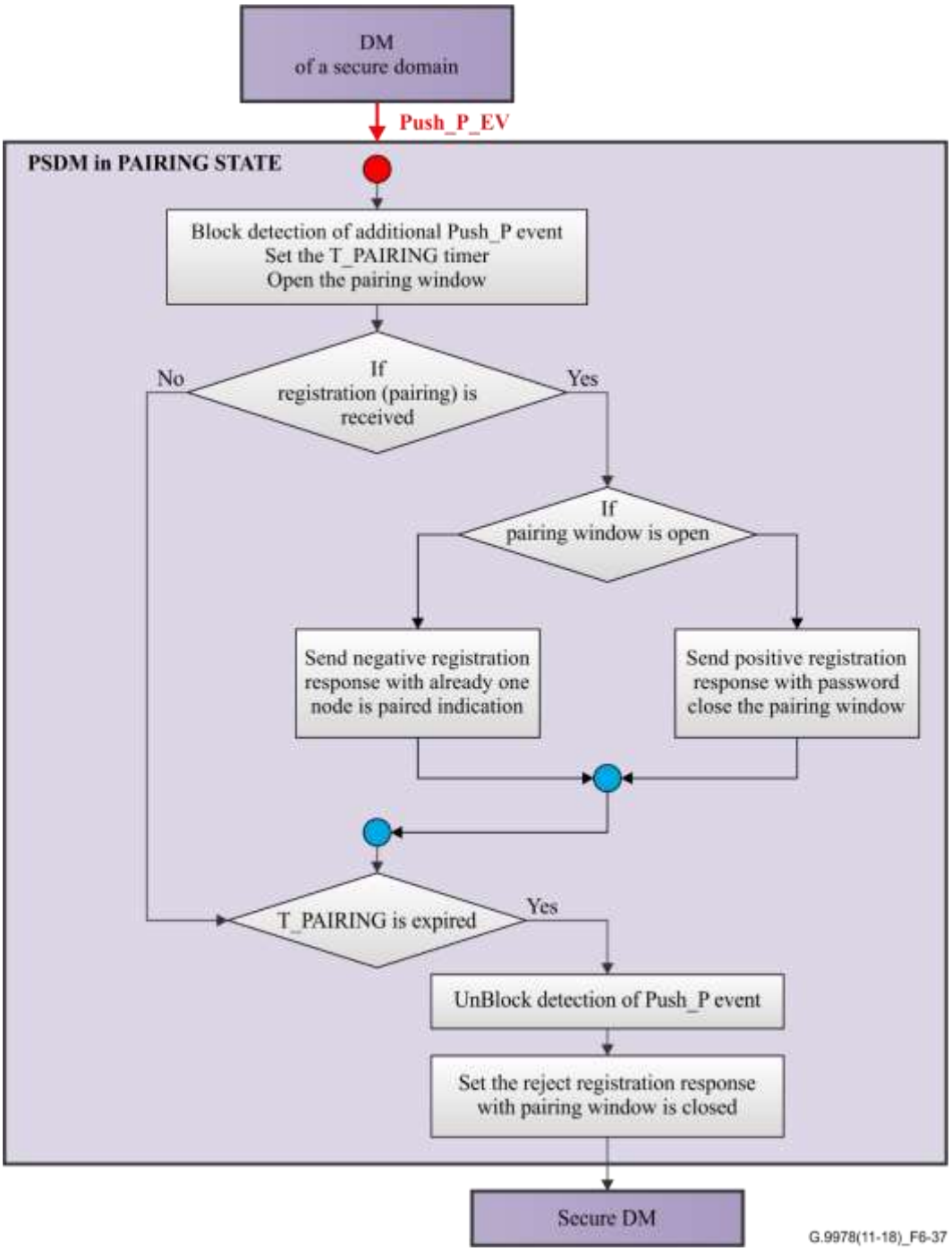

Figure 6-37 – Domain master of a secure domain operation on a PUSH_P event

During the $t_{PAIRING}$ period, the secure DM shall handle only one registration procedure with one joining node and shall respond with a registration response with a negative indication that it has already committed to a pairing procedure with one joining node. During the $t_{PAIRING}$ period, the secure DM shall ignore any new PUSH_P events. After expiry of the $t_{PAIRING}$ period or after the acceptance of a new node into the network, the secure DM shall unblock receipt of the PUSH_P event.

6.2.2.1.4 Informing the domain master about a PUSH_P event

The user may trigger the PUSH_P event on any arbitrary node in an SD and on the joining node in order to start the pairing mechanism. On detection of the PUSH_P event, the triggered EP node in the SD shall send an ADM_NodeReportPUSH_P.ind message (see Table 6-11) to its DM to report about

the PUSH_P event. On receipt of the ADM_NodeReportPUSH_P.ind message, the secure DM shall respond with the ADM_NodeReportPUSH_P.rsp message to the EP node to confirm receipt of the ADM_NodeReportPUSH_P.ind message and immediately open the pairing window to accept a potential registration with a pairing request.

The secure DM will inform the rest of the nodes in the SD by an ADM_PairingWindow.ind broadcast message of the opening and closing of the pairing window.

Figure 6-38 shows the pairing registration protocol via a UI EP node in the single-node pairing mode.

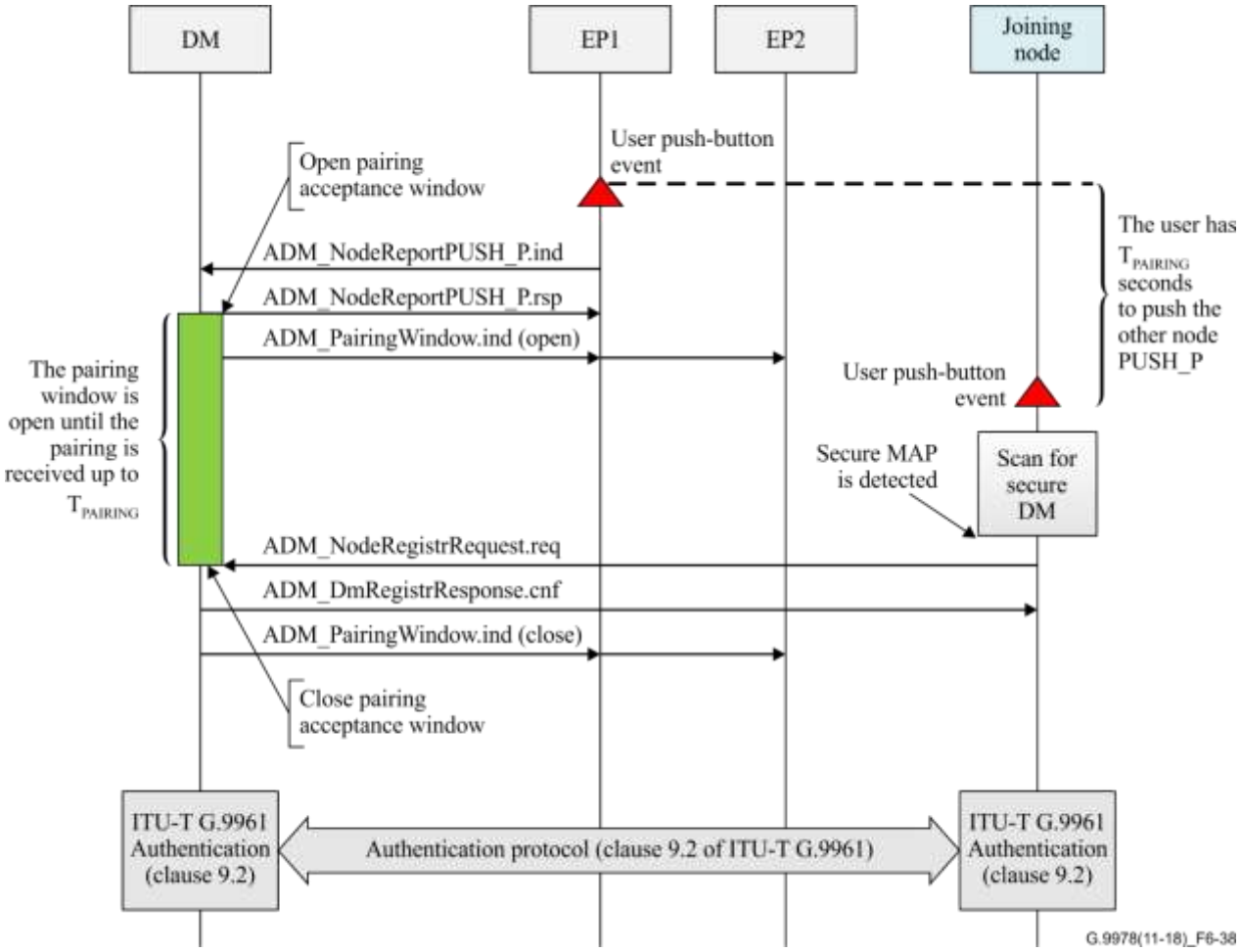

Figure 6-38 – Protocol diagram for pairing registration via a user interface in the single-node pairing mode

6.2.2.1.4.1 Message: ADM_NodeReportPUSH_P.ind

Table 6-11 – Payload of an ADM_NodeReportPUSH_P.ind message

Field	Octet	Bits	Description
OpenDeviceID	0	[7:0]	DEVICE_ID of the EP node that triggered a PUSH_P event.

6.2.2.1.4.2 Message: ADM_NodeReportPUSH_P.rsp

This message has no payload.

6.2.2.1.4.3 Message: ADM_PairingWindow.ind

This is a broadcast message that the DM sends to all nodes in the SD to indicate when the pairing window opens or closes (see Table 6-12). It can be used to manage LEDs or any other indication of the state of the pairing window at the network level.

Table 6-12 – Payload of an ADM_PairingWindow.ind message

Field	Octet	Bits	Description
Code	0	[7:0]	Code is 1 when window closes. Code is 2 when window opens. The rest of values are reserved by ITU.

6.2.2.1.5 Pairing registration protocol in the single-node pairing mode by user confirmation

If the new node powers on in the home network, it will broadcast an ADM_SelfNotify.ind message with its REGID "A" to notify of its existence. If the DM receives this ADM_SelfNotify.ind message, it shall send an ADM_UINewNodeExist.ind message with REGID "A" to the UI node. The AE that is associated with the G.hn UI node will trigger a FLASH_E event to let the user know that a new node is joining the network. At the same time, the pairing window is opened for a $t_{PAIRING}$ period. If the users confirm that the new device can join the secure domain, and on detection of the PUSH_P event within the paring window, the triggered UI node shall send an ADM_UI_MACauthorization.ind message to the DM.

After receiving the indication message, the DM shall open a window to allow registration of this node with REGID "A", only if it has already received the SC_UI_Authorization.req message from the SC indicating that the UI node has been authorized. During this time window, the DM shall broadcast the MAP frames with the RegistrationOffer field set to two and "RegistratioRestrict" field set to REGID "A". The nodes that work with this REGID "A" shall register in the DM.

After the new unconnected node receives the registration confirmation message, it shall send an ADM_SecureDomain.req message, which includes the PW for authentication, to the authorized nodes that have registered on it. The DM shall also distribute a MAC authorization information subfield to the Medium Access Plan-Default (MAP-D) frames for 120 s, which includes collected information about neighbouring nodes that have registered in an NSD. A node in an NSD shall monitor MAP-D frames from neighbouring domains and, if it detects that its information is included in the MAC authorization information subfield in the MAP-D frames, it shall leave the NSD and register in the SD.

On receipt of the ADM_SecureDomain.req message, the receiving node shall confirm receipt by replying with an ADM_SecureDomain.cnf message. The receiving node shall use the PW and DN to complete authentication with the SC. The nodes that are not working with the REGID "A" shall be rejected by the DM.

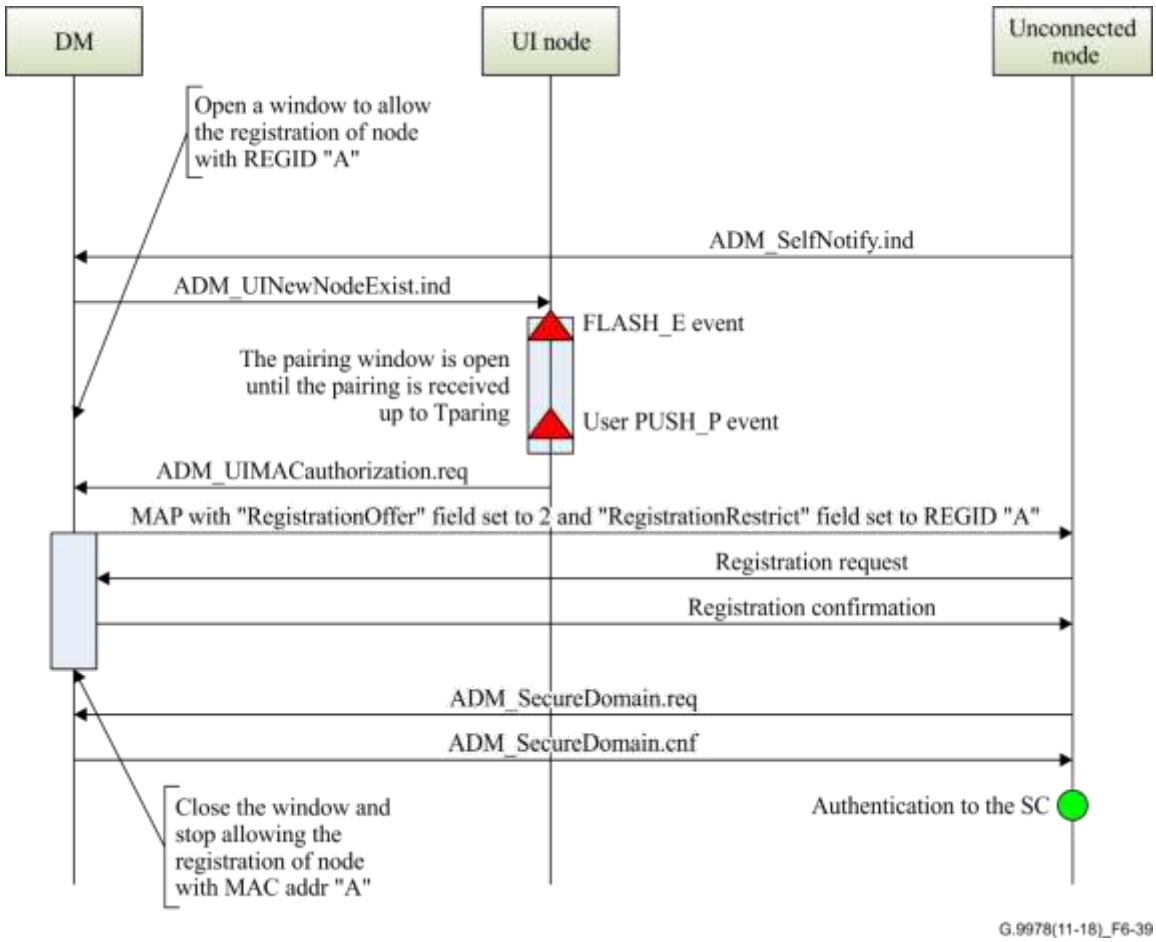

Figure 6-39 – Pairing registration protocol diagram in the single-node pairing mode by user confirmation

6.2.2.2 Pairing registration in the multi-node pairing mode

The pairing registration procedure under the multi-node pairing mode is used to enable the user to add one or more non-secure nodes to an SD within one $t_{PAIRING}$ period. The pairing registration procedure is the same as in single-node pairing mode except that the DM shall close the pairing acceptance window only after the $t_{PAIRING}$ window period has expired to enable several nodes to register within one $t_{PAIRING}$ period. Figure 6-40 is the protocol diagram of pairing registration in the multi-node pairing mode. In this example, the user triggers the PUSH_P event on one of the secure nodes of the SD, which informs its DM about it.

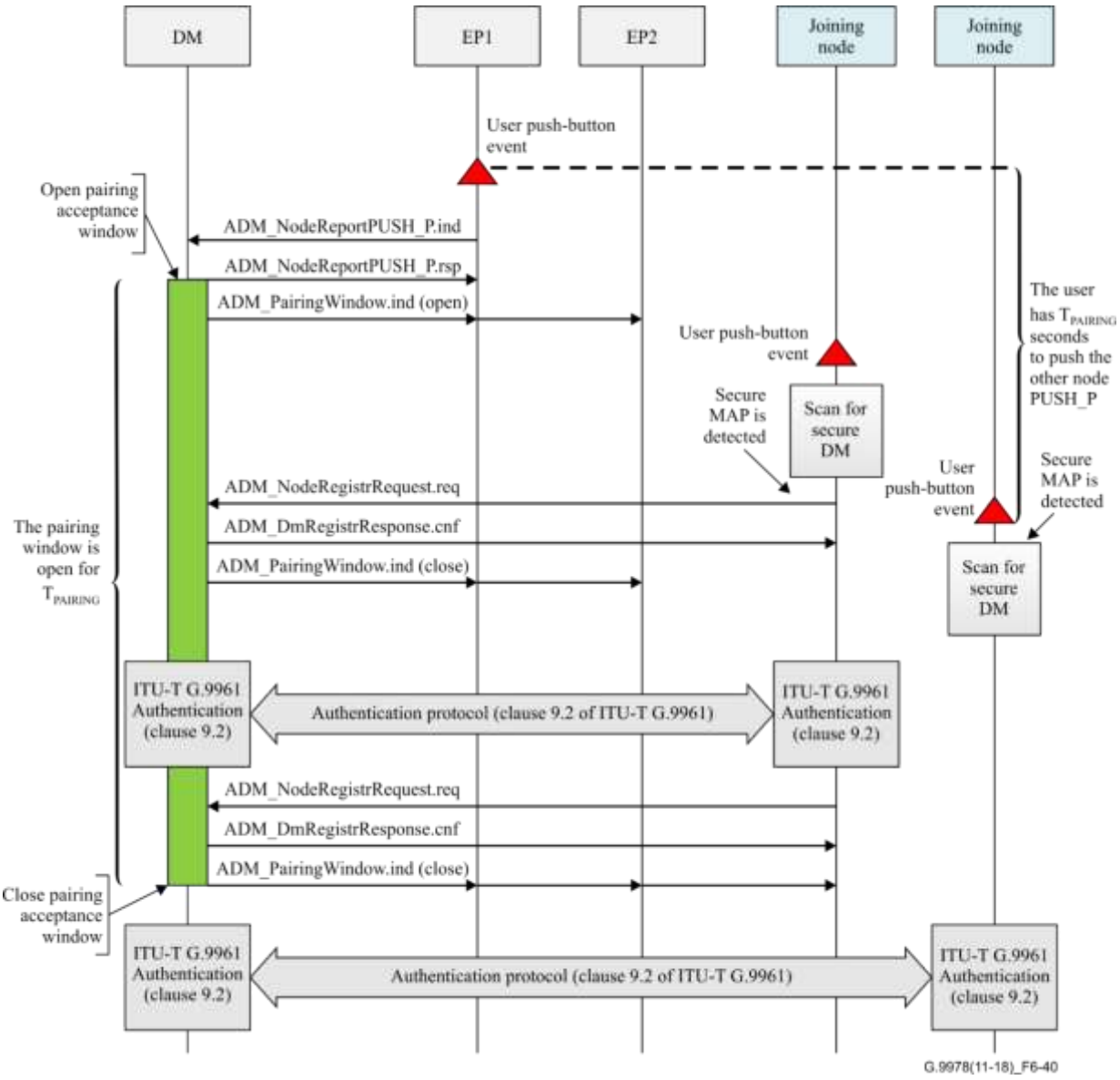

Figure 6-40 – Protocol diagram of pairing registration in the multi-node pairing mode

On receipt of the PUSH_P event, the DM shall open the pairing window for a period of $t_{PAIRING}$.

On receipt of an ADM_NodeRegistrRequest.req message, the DM shall process the registration request and shall reply within REG_RESP_TIME to the requesting node with an ADM_DmRegistrResponse.cnf message.

If the DM receives the registering request message while it is within a pairing window, the ADM_DmRegistrResponse.cnf message shall include the following fields:

– a status flag with a success registration indication;

– a PW needed for the authentication procedure (clause 9.2 of [ITU-T G.9961]);

– a non-zero DEVICE_ID for the registering node assigned by the DM;

– all other relevant configuration data as specified in [ITU-T G.9961].

On receipt of the ADM_DmRegistrResponse.cnf message, the registering node shall identify the ADM_DmRegistrResponse.cnf message based on its REGID field and adopt the DN of the domain that replied positively and its new assigned DEVICE_ID. The registering node shall use the PW included in the ADM_DmRegistrResponse.cnf message for the authentication procedure as specified in clause 9.2 of [ITU-T G.9961].

If the DM receives a registration request while its pairing window is closed, it shall reject the registration request by replying to the joining node with a ADM_DmRegistrResponse.cnf message that contains the status flag set to zero and an extended rejection code 0x3 that indicates that the registration request is rejected for the reason that "pairing window is closed" and the DEVICE_ID shall be set to zero.

During the $t_{PAIRING}$ period, the DM shall block any other PUSH_P events and shall ignore any new PUSH_P events. After expiry of the $t_{PAIRING}$ period, the DM shall unblock receipt of new PUSH_P event and close the pairing acceptance window.

Figure 6-41 shows the state machine of a secure DM after a PUSH_P event.

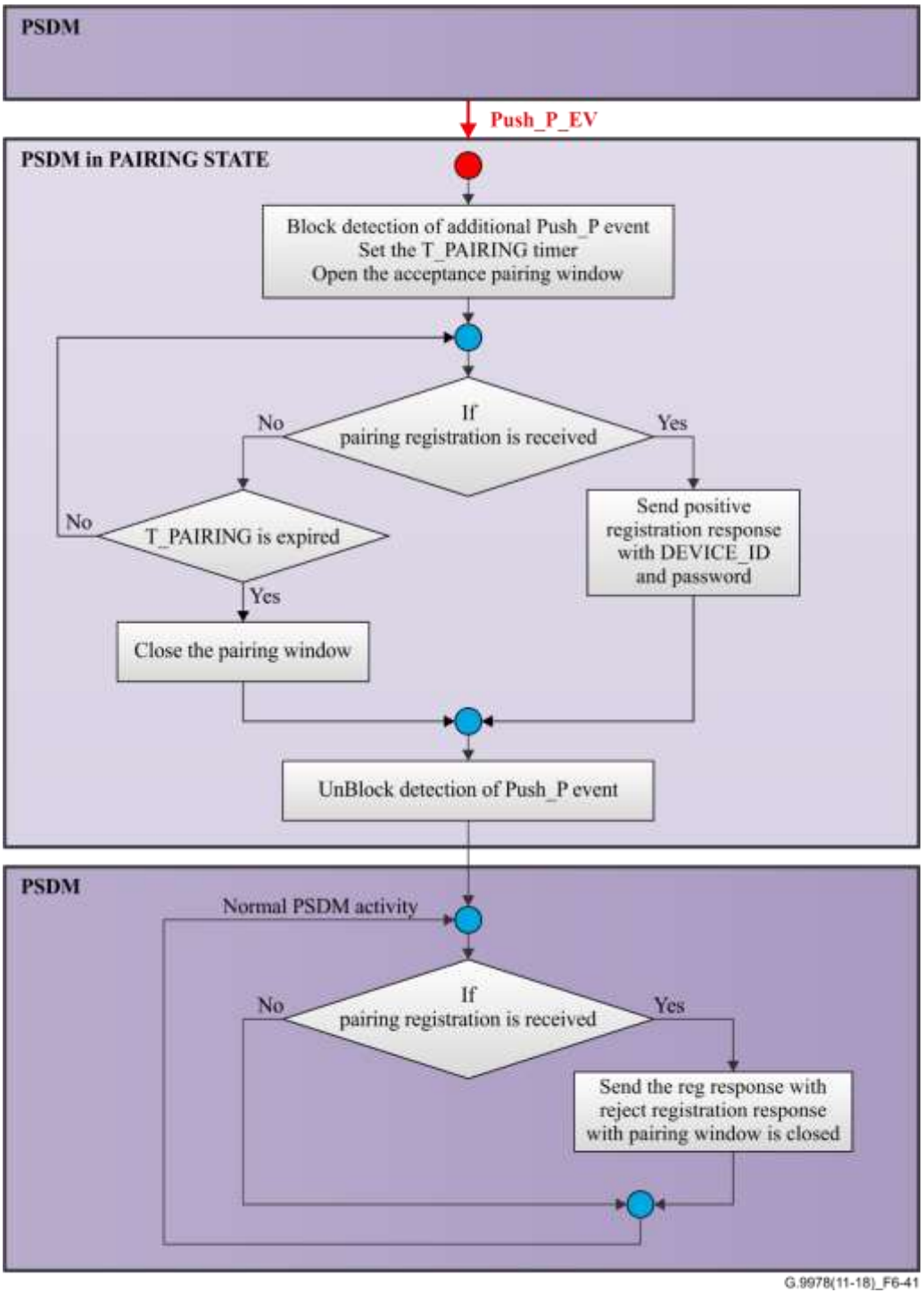

Figure 6-41 – State machine of a secure domain master after a PUSH_P event

6.2.2.2.1 Conversion of a non-secure domain to a secure domain in the multi-node pairing mode

The multi-node pairing mode enables the user to convert an entire NSD to an SD by triggering the PUSH_P event on all nodes of the domain. Figure 6-42 illustrates the way an NSD is converted into an SD in multi-node pairing mode.

NOTE 1 – Figure 6-42 shows a particular sequence of PUSH_P events. However, any other sequence of PUSH_P events is also valid.

NOTE 2 – The sequence in Figure 6-42 makes use of the DM and EP state alternation mechanism described in clause 6.2.2.1.1.

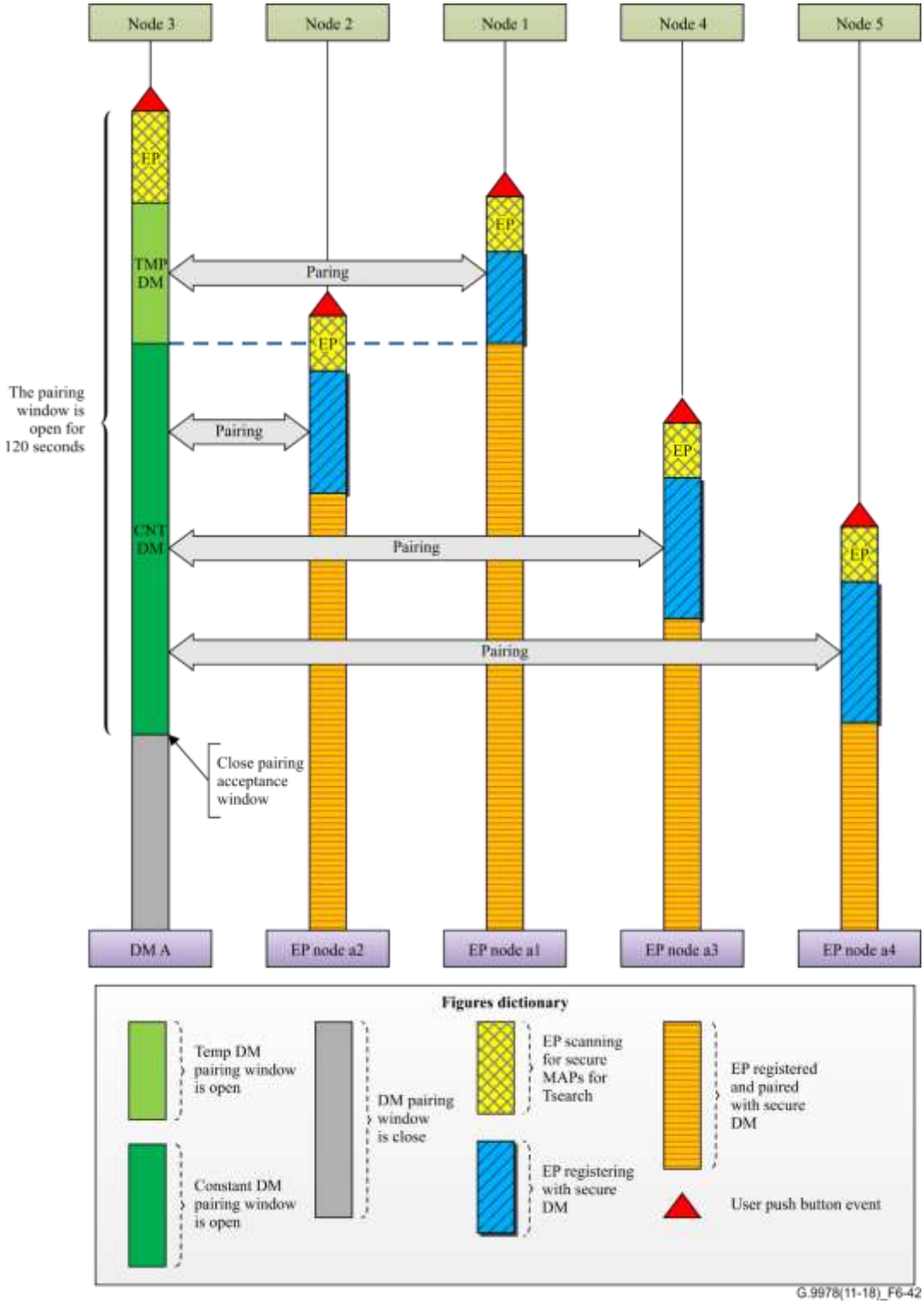

Figure 6-42 – Protocol diagram of pairing registration in the multi-node pairing mode

In Figure 6-42, node 3 is the first to trigger the PUSH_P event. It starts scanning for an SD. After t_0 it becomes a temporary DM of a new SD (DM A). Node 1 is the second to be triggered by the PUSH_P event; it starts scanning for an SD and it detects MAPs transmitted by temporary DM A. Then node 1 registers with DM A and after completion of the registration procedure becomes an EP node in domain A (as node a1). Then node 2 is the third to be triggered by the PUSH_P event. It starts scanning for an SD and it detects MAPs transmitted by temporary DM A. Node 2 conducts the registration procedure with DM A and after completion of the registration procedure becomes an EP node in domain A (as node a2). Then node 4 is triggered by the PUSH_P event and does the same and becomes an EP node in domain A (as node a3). Then node 5 is triggered by the PUSH_P event and it does the same and becomes an EP node in domain A (as node a4). Successful completion of the multi-node pairing procedure results in a new SD A.

During multi-node pairing procedures where pairing is performed among several nodes simultaneously, faulty cases where several SDs are created may occur. This can happen because during the pairing open window, more than one node might become a temporary DM, with a unique random DN, some nodes register with one temporary DM while other nodes register with another temporary DM. This kind of scenario leads to creation of two SDs with two different DNs as illustrated in Figure 6-43.

NOTE 3 – Figure 6-43 shows a particular sequence of PUSH_P events. However, any other sequence of PUSH_P events is also valid.

NOTE 4 – The sequence in Figure 6-43 makes use of the DM and EP state alternation mechanism described in clause 6.2.2.1.1.

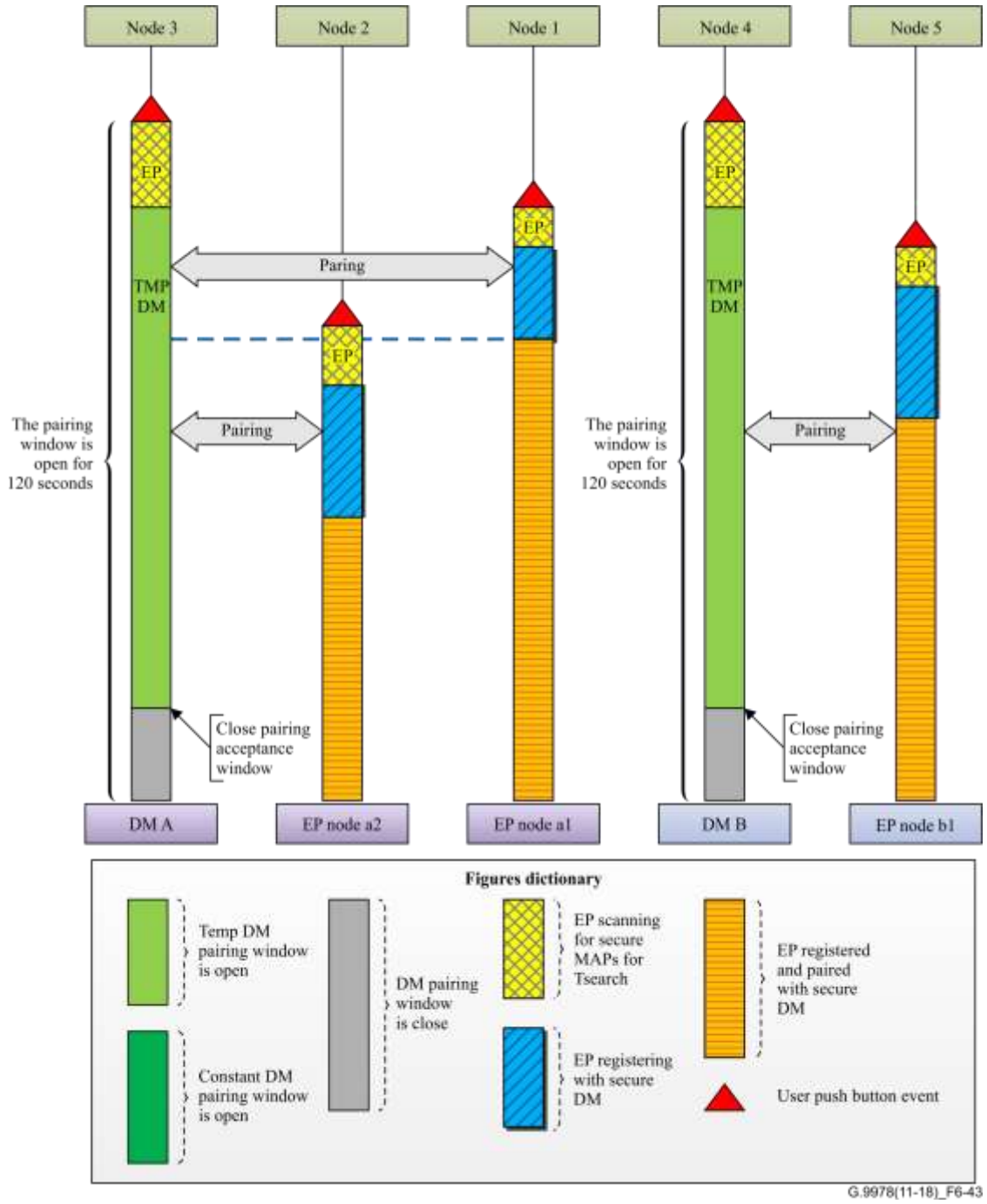

Figure 6-43 – Multi-node pairing procedure that results in two secure domains

In Figure 6-43, node 3 becomes temporary DM of domain A and node 4 becomes temporary DM of domain B. Node 1 registers on temporary DM A and becomes EP node a1 in SD A. Node 2 registers on temporary DM A and becomes EP node a2 in SD A. Node 5 registers on temporary DM B and becomes EP node b1 in SD B.

In order to avoid the problem described in the previous paragraphs, each temporary DM that completes a registration procedure successfully with one of its nodes may follow the procedure described in clause 6.2.2.2.1.1.

6.2.2.2.1.1 Merging of secure domains with temporary DMs

If this procedure is followed, the DM shall not become immediately a permanent DM, but it shall continue acting as a temporary DM until the expiry of the current pairing window. The temporary DM following the procedure described in clause 6.2.2.1.1 shall allocate a dedicated TXOP for the registered EP for scanning and pairing with other potential DMs. This temporary DM shall also use this TXOP to scan for other potential DMs. During this time, if the temporary DM detects MAPs from other temporary DMs, it shall register on the detected DM's domain as an EP node. In this procedure, any registered node that loses its temporary DM shall scan for MAPs from other DM and shall try to register with it.

Figure 6-44 illustrates the merge procedure.

NOTE – Figure 6-44 shows a particular sequence of PUSH_P events. However, any other sequence of PUSH_P events is also valid.

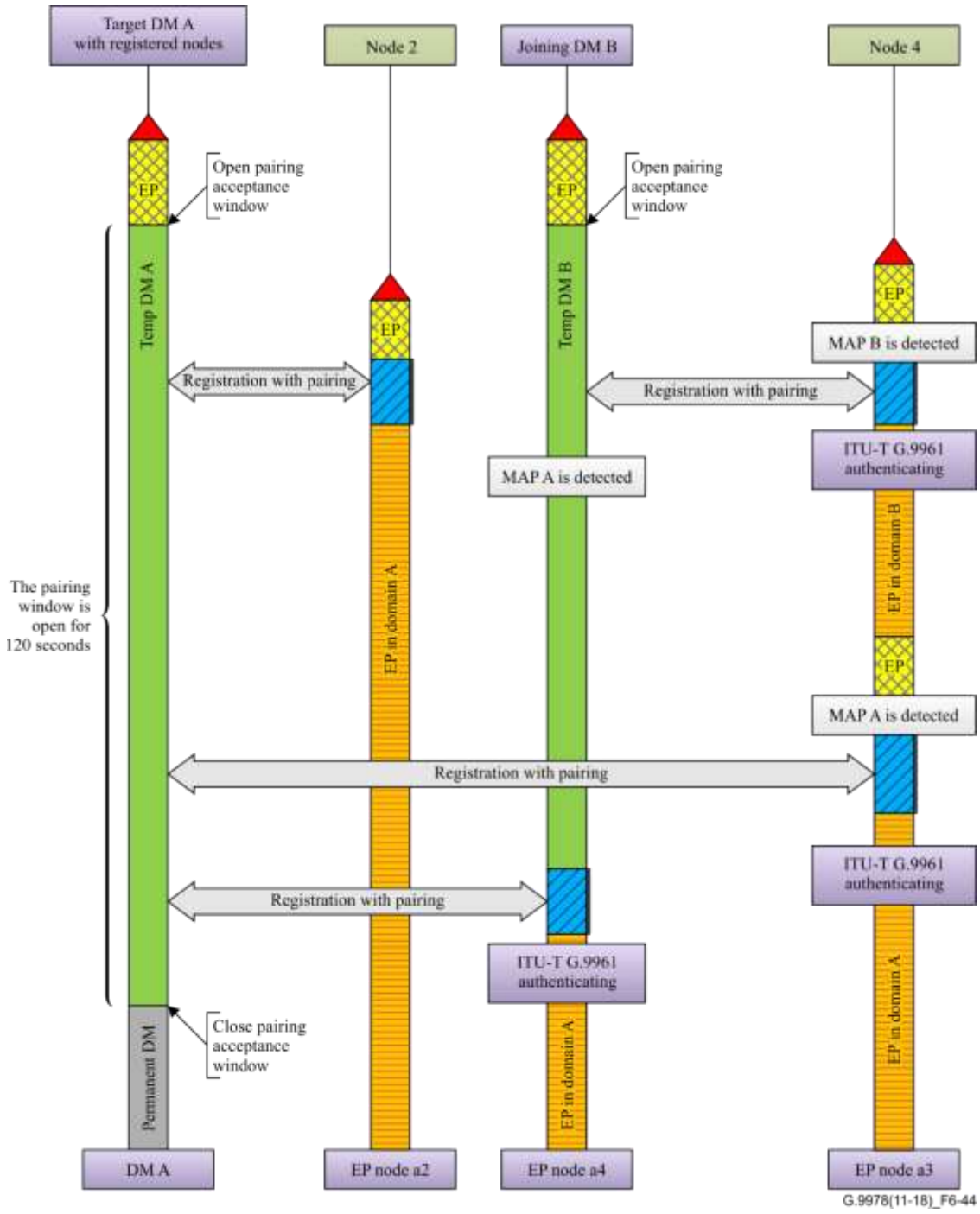

Figure 6-44 – Multi-node pairing procedure that results in two secure domains

6.3 Secure admission through a passphrase-based procedure

In this procedure, the user sets up an SD by entering a passphrase (made up of ASCII characters) into each of the nodes it wants to connect to the domain. This passphrase is converted into a PW that is then converted into a domain-wide key that is used for encryption of communications between the nodes of the domain.

6.3.1 Use cases

This clause describes use cases for secure admission through a passphrase-based procedure. See Table 6-13.

Table 6-13 – Use cases for secure admission through a passphrase

Use case	Description	Comments
1	A user creates a secure domain with two nodes	The user creates a secure domain with two nodes by configuring them to work in secure mode
2	Join a node to existing secure domain	Every node for addition to the secure domain requires configuration with the same secure parameters as specified in the existing secure domain

6.3.1.1 Use case 1 – A user creates a secure domain with two nodes

The user sets up an SD by configuring the same passphrase (ASCII) into each of the nodes it wants to connect to the domain.

The user configures node 1 with the following parameters.

– Secure mode – The security mode of the node may already be set to "secure mode" by the node's vendor.

– DN – The user may either configure the domain to use a non-default DN of its choosing, or it may use the default DN already specified by the node's vendor (i.e., the user does not need to configure the DN).

– User-specified passphrase in ASCII format – The way the user introduces the passphrase is vendor discretionary.

After configuring the passphrase, the node shall derive a PW from the passphrase as specified in clause 6.3.2.1. An encryption key shall then be derived from the PW as specified in clause 6.3.2.2, as shown in Figure 6-45.

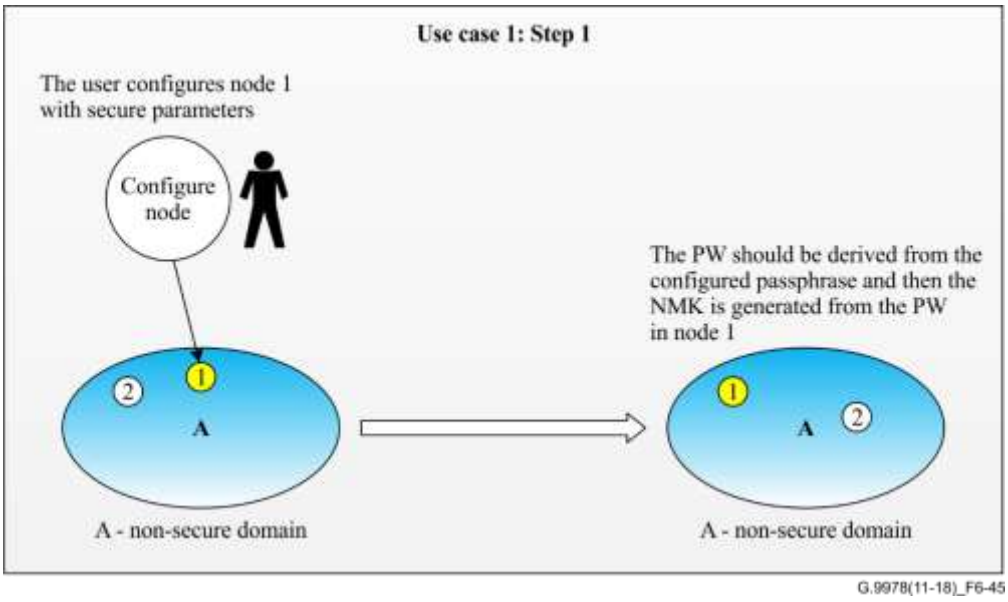

Figure 6-45 – Step 1: A user creates a secure domain with two nodes

The user configures node 2 with the following parameters.

– Secure mode – The security mode of the node may already be set to "secure mode" by the node's vendor.

– DN – The user may either configure the domain to use a DN of its choosing, or it may use the name already specified by the node's vendor (i.e., the user does not need to configure the DN).

– User-specified passphrase in ASCII format – The way the user introduces the passphrase is vendor discretionary.

After configuring the passphrase, the node shall derive a PW from the passphrase as specified in clause 6.3.2.1. An encryption key shall then be derived from the PW as specified in clause 6.3.2.2.

Node 1 and node 2 establish an SD as shown in Figure 6-46.

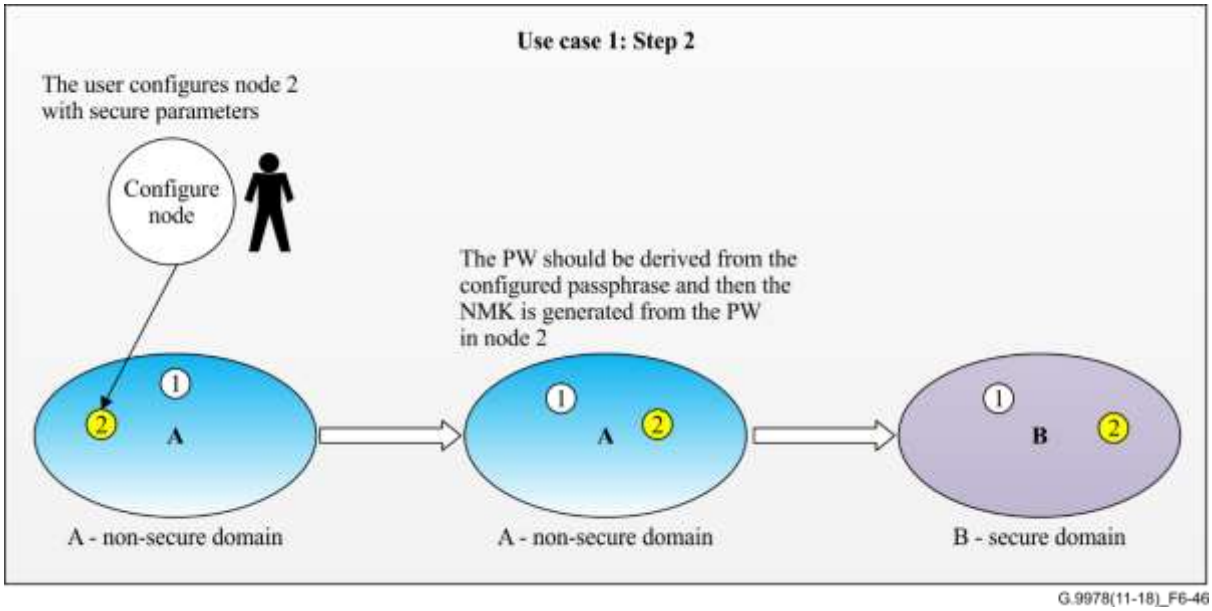

Figure 6-46 – Step 2: A user creates a secure domain with two nodes

6.3.1.2 Use case 2 – Join a node to an existing secure domain

This use case refers to a scenario where the user wants to add an additional node to an SD that was created by the passphrase method.

The user configures node 3 with the secure parameter as specified in clause 6.3.1.1.

After configuring the passphrase, the node shall derive a PW from the passphrase as specified in clause 6.3.2.1. An encryption key shall then be derived from the PW as specified in clause 6.3.2.2.

Figure 6-47 illustrates use case 2 procedures.

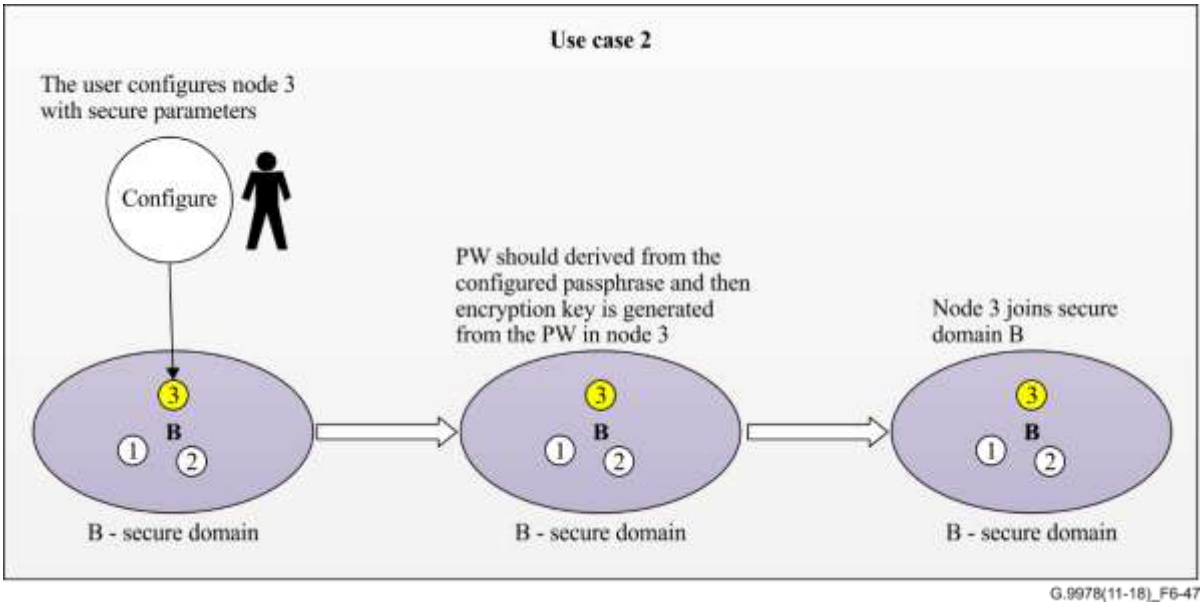

Figure 6-47 – Join a node to an existing secure domain

6.3.2 Secure admission description

The user sets up an SD by configuring the same passphrase (ASCII) into each of the nodes it wants to connect to the domain.

In order to set up an SD, users need to perform the following configuration for each node they wish to connect to the SD.

1) Configure the node to work in secure mode. The security mode of the node may already be set to "secure mode" by the node's vendor.
2) Configure a DN. Users may either configure the domain to use a DN of their choosing or they may use the name already specified by the node's vendor (i.e., the user does not need to configure the DN).
3) The user introduces a user-specified passphrase to the node in ASCII format. The way the user introduces the passphrase is vendor discretionary.

After configuring the passphrase, the node shall derive a PW from the passphrase as specified in clause 6.3.2.1. An encryption key shall than be derived from the PW as specified in clause 6.3.2.2.

An EP node configured to secure mode shall only try to register on a DM indicating it is operating in secure mode (indicated in MAP-Ds by the bit of the security-related domain info subfield, see clause 8.8.5.16 of [ITU-TG.9961]) and having the same configured DN.

6.3.2.1 Generation of the password from the user-introduced passphrase

– The passphrase is a user-specified chain of characters with the following characteristics.
  - Chain length: 12 ASCII characters (C0C1C2…CN…C11)
  - Valid characters: [a-z];[A-Z];[0-9]
– The PW is a 96-bit binary chain: (b0b1…b95)

Each character of the passphrase is converted into its 8-bit binary equivalent following [ISO/IEC 8859-1], starting from C0. The MSB of the binary representation corresponds to the first bit of the byte:

Example

– Passphrase: GhnCertf2013
– ASCII codes:

Character	**G**	**h**	**n**	**C**	**e**	**r**	**t**	**f**	**2**	**0**	**1**	**3**
ASCII code (hex)	47	68	6E	43	65	72	74	66	32	30	31	33
ASCII code (bin)	01000111	01101000	01101110	01000011	01100101	01110010	01110100	01100110	00110010	00110000	00110001	00110011

– PW:
0100011101101000**01101110**01000011**01100101**01110010**01110100**01100110**00110010**0
01100000**00110001**00110011

6.3.2.2 Generation of the domain-wide key from the password

The network membership key (NMK) is derived from the PW by:

– the first 96 bits of the NMK are the 96 bits of the PW.
– the next 32 bits are the repetition of the first 32 bits of the PW.

Example

– *PW*:
0100011101101000**01101110**01000011**01100101**01110010**01110100**01100110**00110010**0
01100000**00110001**00110011

– *NMK*
0100011101101000**01101110**01000011**01100101**01110010**01110100**01100110**00110010**0
01100000**00110001**00110011**01000111**01101000**01101110**01000011

6.4 Admission through the auto-pairing mechanism

This clause defines a pairing method that enables establishment of an SD that requires minimal user intervention.

This pairing method is based on automatic flow where a node that is not paired triggers the PUSH_P event automatically once it has been plugged into the network and tries to create or join an SD within a pairing window time.

6.4.1 Use cases

This clause describes the use cases for secure admission through auto-pairing. See Table 6-14.

Table 6-14 – Use cases for secure admission through auto-pairing

Use case	Description	Comments
1	A user creates a secure domain with multi-nodes	The nodes that are plugged into the network during the pairing window time shall create a secured domain
2	A user adds a node to an existing domain after the pairing window time has expired	The nodes that are plugged into the network after the pairing window time has expired shall move to the unconnected state
3	Fault case – The user plugs only one node into the network	The node will open the auto-pairing timer and once the timer has expired the node should move into the unconnected state

NOTE – The blue bubbles in Figures 6-44 and 6-45 refer to nodes that are in unconnected mode or nodes in an NSD.

6.4.1.1 Use case 1 – A user creates a domain with multi-nodes

In this case, in order to join nodes to an existing SD the user has to plug all nodes into the network within one pairing window time.

An SD with nodes 1, 2, 3 and 4 is established as illustrated in Figure 6-48.

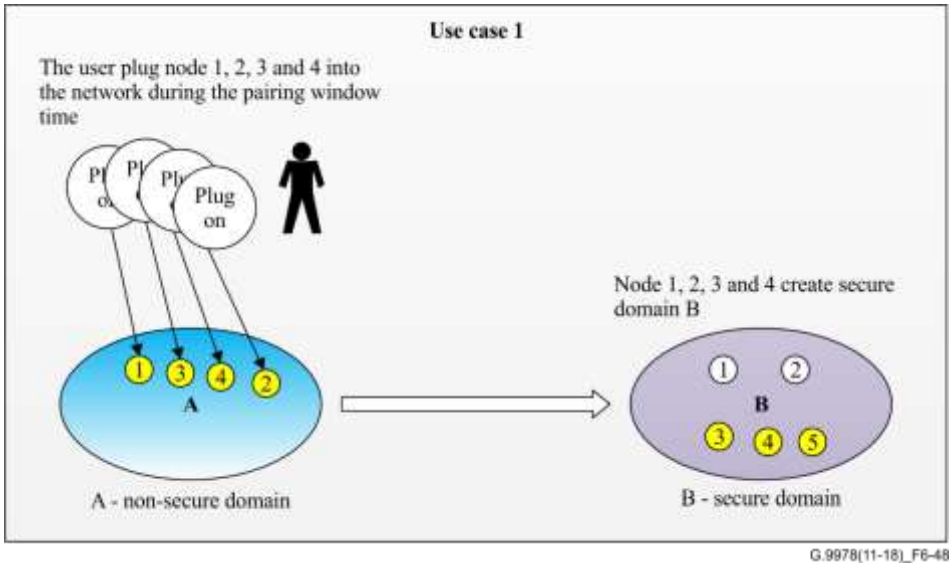

Figure 6-48 – A user creates a domain with multi-nodes

6.4.1.2 Use case 2 – A user adds a node to an existing secure domain after the pairing window time has expired

In this case, the user plugs node 3 into the network after the pairing window of the SD has expired.

If node 3 does not find any secure DM with an auto-pairing window open, it shall move to the unconnected state as illustrated in Figure 6-49.

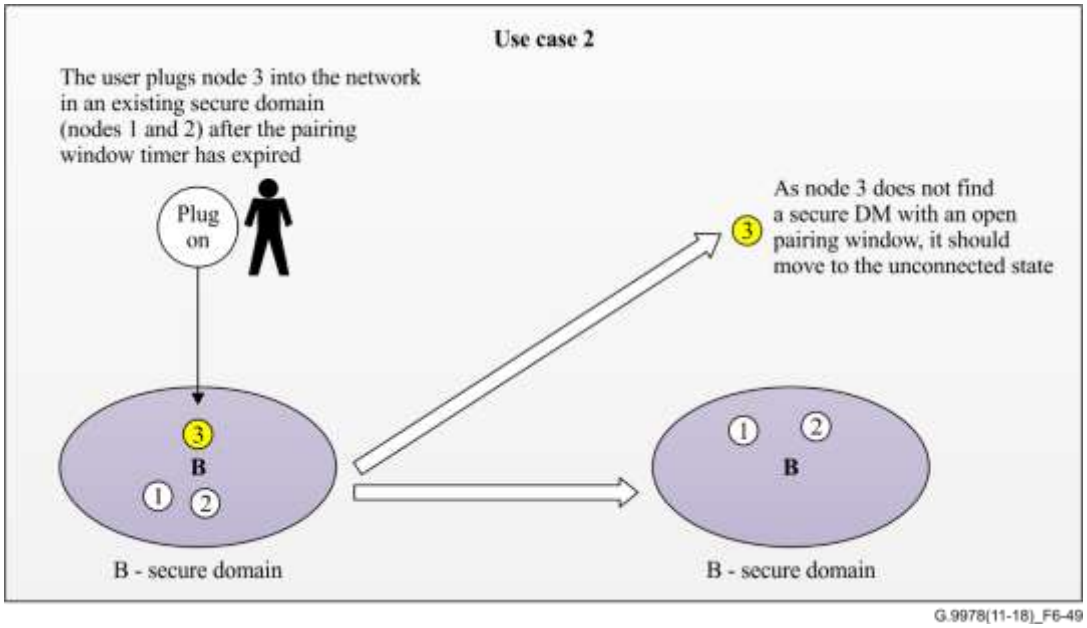

Figure 6-49 – A user adds a node to an existing domain after the pairing window time has expired

In order to complete the admission process to SD B, node 3 shall follow the procedure described in clause 6.2.1.2.1.

6.4.1.3 Use case 3 – Fault case – The user plugs only one node into the network

In this fault case, the user plugs only one node into the network.

In this fault case, nothing should happen. This case is considered to be a faulty case because the user does not complete the pairing procedure. In this case, after the pairing window has expired the node shall move to the unconnected state, as illustrated in Figure 6-50.

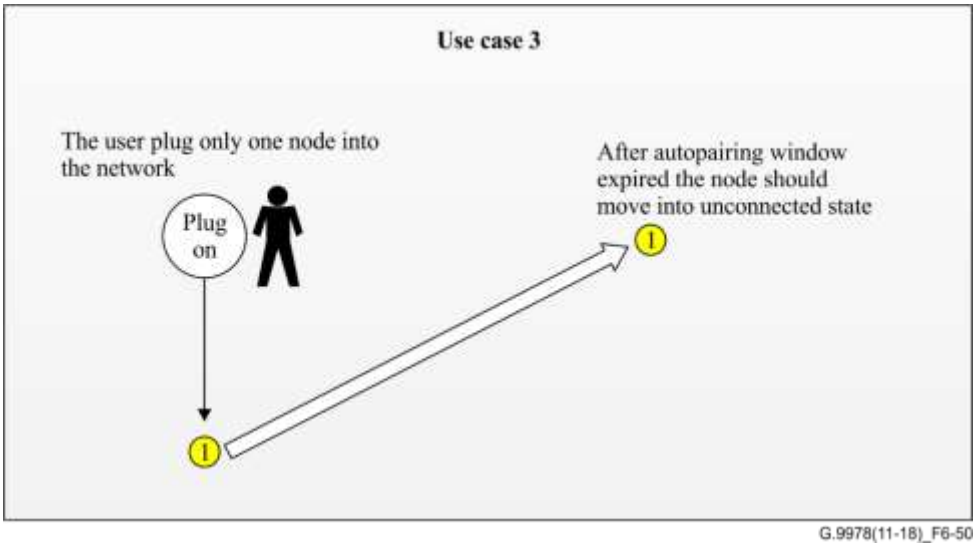

Figure 6-50 – Fault case – The user plugs only one node into the network

6.4.2 Secure admission by pairing in an auto-pairing scenario

A pairing mechanism in an auto-pairing scenario enables the user to convert an NSD to an SD or to add one or more nodes to an SD, just by plugging them into the network.

Table 6-15 lists system parameters for the pairing mechanism in an auto-pairing scenario.

Table 6-15 – Parameters for pairing mechanism in an auto-pairing scenario

Parameter	Description	Medium			
		Power-line baseband	**Coax BB**	**Coax RF**	**Phone line**
$t_{PAIRING}$	Pairing window that starts after a PUSH_P event is triggered, after plugging the node into the network. During this period, the DM shall confirm the registration pairing request	60-300 s	60-300 s	60-300 s	60-300 s
T_EP_INTERVAL	The interval during which a pairing node acts as an EP trying to pair with a secure domain until it shall alternate to a temporary domain master	Random value in the range 0-10 s	Random value in the range 0-10 s	Random value in the range 0-10 s	Random value in the range 0-10 s
T_TMPDM_INTERVAL	Period of time during which a node in a pairing procedure shall act as a temporary domain master before it alternates to an endpoint node for scanning	Random value in the range 4-8 s	Random value in the range 4-8 s	Random value in the range 4-8 s	Random value in the range 4-8 s
NOTE – The value of $t_{PAIRING}$ is vendor discretionary and is usually fixed by an external entity (e.g., HomeGrid Forum, [b-HomeGrid]).					

The procedure for the auto-pairing scenario shall be the same as specified in clause 6.2.2.1 except for the following differences:

1) the pairing window time ($t_{PAIRING}$) shall be as specified in Table 6-15;
2) the pairing event is triggered once the node (that is not paired) has been plugged into the network.

6.4.2.1 Pairing registration in an auto-pairing scenario

The protocol of the pairing registration in an auto-pairing scenario shall work similarly to that specified in clause 6.2.2.2, except for the following two differences:

1) the pairing window time ($t_{PAIRING}$) should be as specified in Table 6-15;
2) the pairing event is triggered once the node (that is not paired) is plugged into the network.

The pairing registration protocol diagram is presented in Figure 6-51.

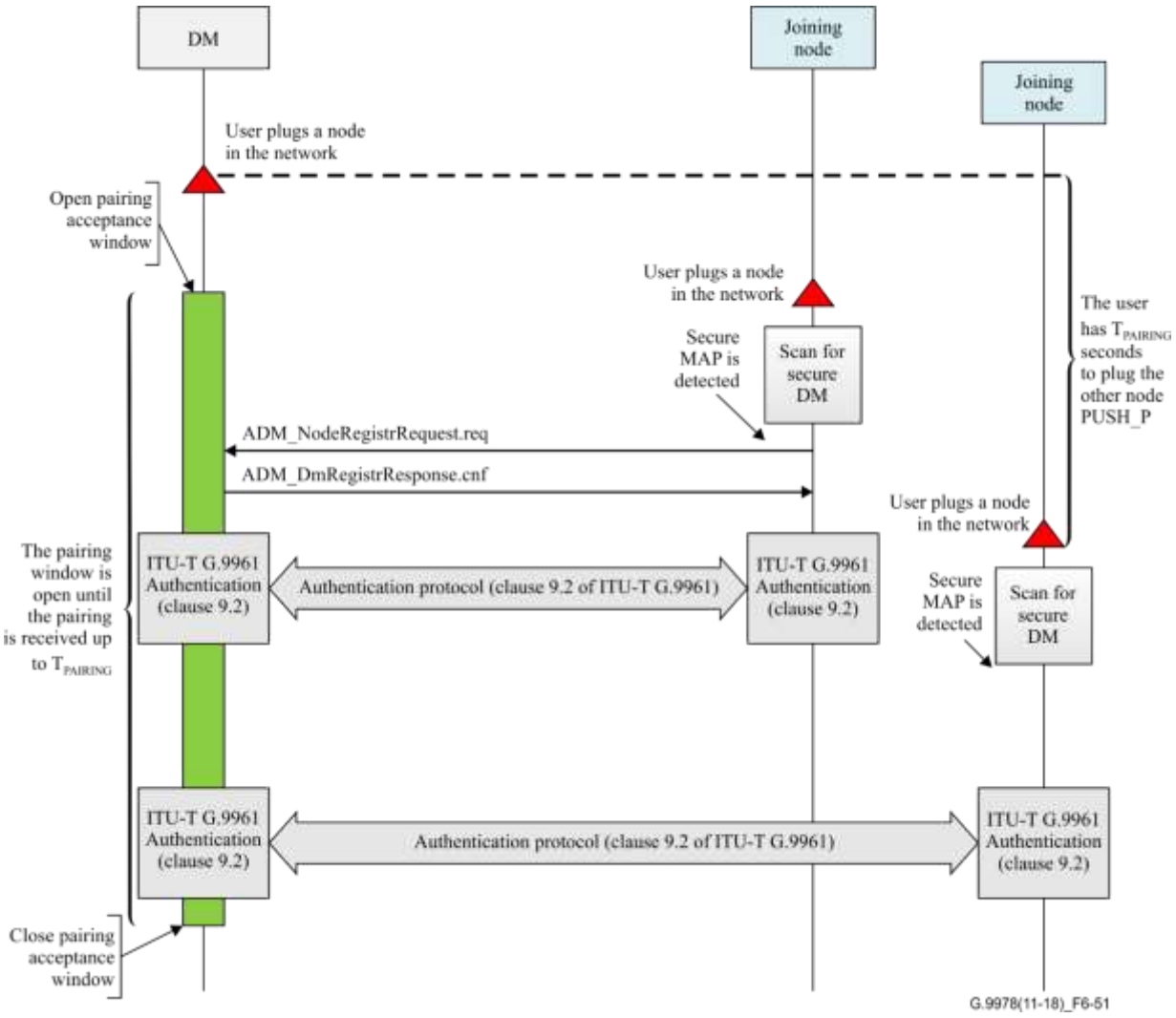

Figure 6-51 – Pairing registration process in an auto-pairing scenario

On plugging a DM into the network, it shall open the pairing window for a period of $t_{PAIRING}$.

On receipt of an ADM_NodeRegistrRequest.req message, the DM shall process the registration request and shall reply within REG_RESP_TIME to the requesting node with an ADM_DmRegistrResponse.cnf message.

If the DM receives the registering request message while it is within a pairing window, the ADM_DmRegistrResponse.cnf message shall include the following fields:

– a status flag with a success registration indication;

– a PW needed for the authentication procedure (see clause 9.2 of [ITU-T G.9961]);

– a non-zero DEVICE_ID for the registering node assigned by the DM;

– all other relevant configuration data as specified in [ITU-T G.9961].

On receipt of the ADM_DmRegistrResponse.cnf message, the joining node shall identify the ADM_DmRegistrResponse.cnf message based on its REGID field and adopt the DN of the domain that replied positively and its new assigned DEVICE_ID. The joining node shall use the PW included in the ADM_DmRegistrResponse.cnf message for the authentication procedure as specified in clause 9.2 of [ITU-T G.9961].

If the DM receives a registration request while its pairing window is closed, it shall reject the registration request by replying to the registering node with a ADM_DmRegistrResponse.cnf message that contains the status flag set to zero and an extended rejection code 0x3 that indicates that

the registration request is rejected for the reason that "pairing window is closed" and the DEVICE_ID shall be set to zero.

During the $t_{PAIRING}$ period, the DM shall block any other PUSH_P events and shall ignore any new PUSH_P events. After expiry of the $t_{PAIRING}$ period, the DM shall unblock receipt of new PUSH_P events and close the pairing acceptance window.

6.4.2.2 Conversion of a non-secure domain to a secure domain in an auto-pairing scenario

The multi-node pairing mode enables the user to convert an entire NSD to an SD by triggering a PUSH_P event on all the nodes of the domain. This procedure in an auto-pairing scenario shall be the same as that specified in clause 6.2.2.2.1, except for the following differences:

1) the pairing window time ($t_{PAIRING}$) shall be as specified in Table 6-15;

2) the pairing event is triggered once the node (that is not paired) has been plugged into the network.

7 Secure admission methods selection

7.1 Information on secure supported admission methods

The DM of the domain is the entity responsible for selecting which admission methods are accepted for a node to request the admission in the domain. The default accepted secure methods for a domain shall be the secure admission methods supported by the first DM since creation of the domain. The new DM shall not change the accepted admission methods when the DM changes.

The DM shall publish the list of accepted admission methods through the AdmissionMethodsInfo subfield: the security-related auxiliary information field of the MAP-D. The contents of this field shall follow the format presented in Table 7-1.

Table 7-1 – Format of AdmissionMethodsInfo subfield

Field	Octet	Bits	Description
GeneralMethods	0	[7:0]	Bitmap representing different methods that are accepted to admit a new node into the domain. Bit 0 represents the LSB. When the bit is set to one, the corresponding methods are accepted as a valid method. When the bit is set to zero, the method is not accepted as a valid method. Bit 0: Admission through passphrase (see clause 6.3). Bit 1: Admission through Auto-pairing (see clause 6.4). Bit 2-7: Reserved by ITU-T (Note)
PushButtonMethods	1	[7:0]	Bitmap representing different methods that are accepted to admit a new node into the domain. Bit 0 represents the LSB. When the bit is set to one, the corresponding methods are accepted as a valid method. When the bit is set to zero, the method is not accepted as a valid method. Bit 0: Admission through generic pairing – Single-node pairing mode (see clause 6.2.2.1). Bit 1: Admission through Autopairing (see clause 6.4). Bit 2: Admission through external authentication (see clause 9.2.8 and Annex D of [ITU-T G.9961]) Bit 3: Admission through native authentication (see clause 9.2 of [ITU-T G.9961]) *Bit ~~2~~4-7: Reserved by ITU-T (Note)*

Table 7-1 – Format of AdmissionMethodsInfo subfield

Field	Octet	Bits	Description
MACMethods	2	[7:0]	Bitmap representing different methods that are accepted to admit a new node into the domain. Bit 0 represents the LSB. When the bit is set to one, the corresponding methods are accepted as a valid method. When the bit is set to zero, the methods is not accepted as a valid method. Bit 0: Admission through MAC authorization (see clause 6.1). Bit 1-7: Reserved by ITU-T (Note)
NOTE – Bits that are reserved by ITU-T shall be set to zero by the transmitter and ignored by the receiver.			

7.2 Interoperability between secure admission methods

This Recommendation specifies multiple secure admission methods for G.hn networks and one or more secure admission methods are allowed to be used in the same domain. The DM shall publish the list of secure admission methods that are used by its domain in the MAP-D (see clause 7.1).

A secure G.hn domain compliant with this Recommendation shall use at least one of the secure admission methods specified in this Recommendation. It may also enable use of multiple secure admission methods simultaneously.

If a node that wants to register in the G.hn domain does not support any of the admission methods specified in the received MAP-D, it shall not try to register on the domain.

The auto-pairing method and passphrase-based method are used to create an SD. The generic pairing method can also be used to create an SD if an SD is not created successfully through an auto-pairing method (i.e., nodes are in the unconnected state).

If auto-pairing is not supported, an NSD may be created. By using any one of the passphrase-based, generic pairing and MAC authorization methods, the NSD can be converted into an SD or parts of the nodes in the NSD can form an SD.

If multiple secure admission methods are used simultaneously, a node and a DM shall act in accordance with the following rules for interoperability:

– a node shall ignore the PUSH_P events that are triggered during the auto-pairing process;

– the unconnected node that is capable of supporting the MAC authorization method and generic method shall search for MAP frames from any SD and be ready to join an SD through a MAC authorization method until it detects the PUSH_P event;

– during the generic pairing window time, if an unconnected node that is capable of supporting the MAC authorization method and generic method detects any secured MAP that contains a MAC authorization information subfield that includes information matching its REGID (see clause 6.1.2.2.2) or any secured MAP with the "Registrationoffer" field set to 1 (see clause 6.1.2.2.1), it shall register in this domain with the "PairingReq" field of the ADM_NodeRegistrRequest.req message set to 1;

– during the generic pairing window time, if a non-secure active node that is capable of supporting the MAC authorization method and generic method detects any secured MAP that contains a MAC authorization information subfield that includes information matching its REGID, it shall register in this domain with the "PairingReq" field of ADM_NodeRegistrRequest.req message set to 1;

– if the DM of an SD that enables the use of both generic pairing and MAC authorization methods is triggered with a PUSH_P event during the MAC authorization process (see clause 6.1.2.2), it shall open a generic pairing window in parallel (see clause 6.2.2);

– for a node that has registered on a secure DM during the MAC authorization process, either by detecting the secure MAP with the "Registrationoffer" field set to 1 (see clause 6.1.2.2.1) or by detecting the secure MAP contains a MAC authorization information subfield that includes information matching its REGID (see clause 6.1.2.2.2), if it is triggered with PUSH_P events, it shall ignore the PUSH_P events;

– a node shall join the domain if it is configured with the passphrase and other related parameters of this domain bypassing other secure admission methods;

– the node that is configured with a passphrase and other related parameters shall ignore the PUSH_P events that are triggered before it become a member of the corresponding domain.

8 Management message OPCODEs

Management message OPCODEs are formatted as 12-bit unsigned integers. Valid values of OPCODEs are presented in Table 8-1.

Table 8-1 – OPCODEs of management messages

Category	Message name	OPC ODE (hex)	Description	MMPL Reference
Secure Admission (B0X)	ADM_UI_MACauthorization.req	B00	Report the DM about the list of authorized nodes	Clause 6.1.2.4.1
	ADM_UI_MACauthorization.cnf	B01	Confirm receiving the ADM_UI_MACauthorization. req message	Clause 6.1.2.4.2
	ADM_SecureDomain.req	B02	Send PW and related parameters to the joining nodes	Clause 6.1.2.4.3
	ADM_SecureDomain.cnf	B03	Confirm receiving the ADM_SecureDomain.req message	Clause 6.1.2.4.4
	ADM_UI_MACauthorization.ind	B04	Report the DM about the MAC authorization event	Clause 6.1.2.4.5
	ADM_UI_MACauthorization.rsp	B05	Response to the ADM_UI_MACauthorization. ind message	Clause 6.1.2.4.6
	SC_UI_Authorization.req	B06	Request to be authorized as a proxy node by the SC for MAC authorization-based secure admission.	Clause 6.1.2.4.7
	SC_UI_Authorization.cnf	B07	Confirm receiving the SC_UI_Authorization.req message	Clause 6.1.2.4.8
	SC_UI_Authorization.ind	B08	Report the new proxy node for MAC authorization-based secure admission.	Clause 6.1.2.4.9
	ADM_SelfNotify.ind	B09	Broadcast by new unconnected node to the network to notify the existence of the new node with its REGID	Clause 6.1.2.4.10

Table 8-1 – OPCODEs of management messages

Category	Message name	OPCODE (hex)	Description	MMPL Reference
	ADM_UINewNodeExist.ind	B0A	Sent from the DM to the UI node to convey the REGID of the new unconnected node	Clause 6.1.2.4.11
Reserved	Reserved	B0B-BFF	Reserved by ITU	

Bibliography

[b-ITU-T G.9960] Recommendation ITU-T G.9960 (2015), *Unified high-speed wireline-based home networking transceivers – System architecture and physical layer specification*.

[b-ITU-T G.9962] Recommendation ITU-T G.9962 (2014), *Unified high-speed wire-line based home networking transceivers – Management specification*.

[b-HomeGrid] HomeGrid Forum (2014), *Any wire. Anywhere. It just works.* Geneva: HomeGrid Forum.
http://www.homegridforum.org/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022