MoCA® Network Password Remote Configuration Application Note

MoCA-PWD-REM-CONFIG-V1.0-200123

IMPORTANT NOTICE. THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN ARE PROVIDED "AS IS" AND "WITH ALL FAULTS". NEITHER MoCA® NOR ANY MEMBER OF MoCA MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER WITH RESPECT TO (A) THIS DOCUMENT, (B) ANY PRODUCT THAT IS DEVELOPED OR MANUFACTURED IN ACCORDANCE WITH THE SPECIFICATIONS IN THIS DOCUMENT OR (C) THE INTEROPERABILITY OF ANY SUCH PRODUCT WITH ANY OTHER PRODUCT. MoCA AND MoCA MEMBERS DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NON-INFRINGEMENT AND TITLE. NEITHER MoCA NOR ANY MEMBER OF MoCA MAKES ANY REPRESENTATIONS OR WARRANTIES THAT THE CONTENTS OF THE DOCUMENT ARE COMPLETE, ACCURATE OR SUITABLE FOR ANY PURPOSE OR THAT ANY PRODUCT OR OTHER IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS OR OTHER RIGHTS. IN NO EVENT WILL MOCA OR ANY MOCA MEMBER BE LIABLE FOR ANY LOSSES, INVESTMENTS MADE, LIABILITIES, LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OF DATA, INTERRUPTION OF BUSINESS, OR FOR ANY DIRECT, INDIRECT, SPECIAL OR EXEMPLARY, INCIDENTIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, IN CONTRACT, TORT, NEGLIGENCE OR OTHER LEGAL THEORY, INCLUDING WITHOUT LIMITATION IN CONNECTION WITH THE USE OF THIS DOCUMENT, THE INFORMATION CONTAINED HEREIN OR ANY PRODUCT OR IMPLEMENTATION, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. USE OF THIS DOCUMENT IS AT YOUR SOLE RISK. From time to time MoCA may issue improvements, enhancements and other changes to the specification described in this document.

Document Status Sheet

Document Control Number:	MoCA-NPWD-REM-CONFIG-V1.0-200123
Document Title:	MoCA® Network Password Remote Configuration Application Note v1.0
Revision History:	Draft Oct 10, 2019 Issued Jan 23, 2020
Date:	**Jan 23, 2020**
Status:	~~Work in Progress~~ ~~Draft~~ Issued
Distribution Restrictions:	No restrictions

Key to Document Status Codes:

Work in Progress	An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.

1 Introduction & Scope

This Application Note describes how the MoCA® 2.x or MoCA 3.0 Network Password(s) could be remotely configured within a home network without user intervention on an MoCA New Node over the coax medium. This application note applies to MoCA 2.0, MoCA 2.5 and MoCA 3.0 M/P specifications (respectively [1], [2] or [3]).

2 References

[1] MoCA, “MoCA MAC/PHY SPECIFICATION v2.0”, Sept 2019
[2] MoCA, “MoCA MAC/PHY SPECIFICATION v2.5”, Sept 2019
[3] MoCA, “MoCA MAC/PHY SPECIFICATION v3.0”, Sept 2019
[4] MoCA, “MoCA VENDOR ID TABLE v1.1”, March, 2018

3 Prerequisites

MoCA® based devices shipped to Service Provider subscribers must feature a vendor or Service Provider specific unique device ID (such as MAC address, digital certificate, …) for device authentication purpose.

The Pre-Admission Transport Service (specified in their respective MoCA M/P specifications [1], [2] or [3]) must be supported by both the MoCA Network Controller (NC) and the MoCA New Node (NN). Otherwise the NN Password(s) cannot be delivered in-band by the NC over the coax medium:

- If the NN does not support the Pre-Admission Transport, the NN will not be able to send a device authentication request to the NC entity and the password remote delivery sequence will not be initiated.

- If the NC does not support the Pre-Admission Transport, the NN’s device authentication request will be ignored by the NC and the password delivery sequence will abort.

4 Important Security Note about the Selection of the Device Authentication Method

In the MoCA® 2.x and MoCA 3.0 standards, a Preferred NC may not guarantee to be the NC if another Preferred NC with higher NC selection ranking (see NC Selection Ranking Table in [1], [2] or [3]) joins the network or if an another Preferred NC with the same ranking is booted first (however, the MoCA standards provide an indication (optional in MoCA 2.x) to notify the management entity of the presence of multiple Preferred NCs in the network).

This means that the MoCA standards cannot prevent an NC from taking over, recognizing any New Node requesting the password(s) as an "authenticated" device and distributing its Network Password(s) to this node.

The way to prevent a non-Service Provider NC from distributing the Network Password(s) to a Service Provider NN is to select a MUTUAL AUTHENTICATION (2-way authentication) method for the authentication between the Service Provider NN and the Service Provider NC. Contrary to one-way authentication methods in which the NC only authenticates the NN, in 2-way methods both nodes identify the other node: the NC authenticates the NN and the NN also authenticates the NC. The NN triggers the Password Remote Configuration handshake only if it does authenticate the NC.

5 Pre-Admission Transport Service

The MoCA® MAC layer provides a Pre-Admission Transport (PAT) service allowing the upper layers of the MoCA NC to communicate with the upper layers of a MoCA New Node prior to its admission to the MoCA Network.

The Pre-Admission Transport SAP and the transmission of the Pre-Admission Transport messages are specified in the respective MoCA M/P specifications [1], [2] or [3].

The Pre-Admission Transport service's attributes are specified as follows:

- Privacy: The Pre-Admission Transport service messages are transmitted in clear text. The messages are not encrypted by the transport service. Vendor specific information transported by the PAT containers that need to be protected must be encrypted by upper layer entities above the MoCA PAT Service Access Point (specified in the respective MoCA M/P specifications [1], [2] or [3]).

- Message Size and Segmentation: The maximum size of the Pre-Admission Transport Service message is 86 bytes (as specified in the respective MoCA M/P specifications [1], [2] or [3]) with up to 60 bytes of vendor specific information. The Pre-Admission Transport Service does not handle segmentation and reassembly: if the maximum size of PAT message payload is insufficient for the messages of a selected proprietary device authentication protocol, the protocol messages must be segmented by the upper layer entities across multiple Pre-Admission Transport Service messages.

- Message Loss: The Pre-Admission Transport Service is unreliable as MoCA pre admission message transmission could fail on collision and other medium errors. The PAT service does not handle retransmission for message loss: acknowledge and retransmission must be managed by upper layer entities above the MoCA PAT Service Access Point.

- The contents of the MoCA Pre-Admission Transport Service messages are transparent to the MoCA MAC/PHY layers. Upper layer protocol messages presented at the MoCA PAT Service Access Point of the source node will be delivered as is to the MoCA PAT Service Access Point of the destination node.

- Pre-Admission Transport Service messages originated from the NC are broadcasted to all MoCA New Nodes as NNs do not have an assigned Node ID before their admission to the MoCA Network:
    - The peer to peer communication between the upper layers of the NC and a given NN is provided by the message payload encrypted with a pairwise secret key shared by both nodes.

- Pre-Admission Transport Service messages originated from the NN could be unicasted to the NC.

6 Remote Configured Password Attributes

The password(s) delivered in-band over the coax medium are the same MoCA® Network password(s) that could be configured either locally or through any out-of-band method and they obey to the same requirements in the respective MoCA M/P specifications [1], [2] or [3]. The password(s) must be persistent across power cycles and reboots (but factory reset) as described in the respective MoCA M/P specifications.

The MoCA Network Password Remote Configuration is only triggered by New Node's for which Network Password(s) have not been configured after factory reset prior to their admission request to join the MoCA Network.

Whether the MoCA Network password(s) lifetime is limited or not is a function of the management policy above the MoCA layers. Any further change to the Network Password(s) would be the responsibility of the vendor to accept and synchronize the Network Password changes.

7 MoCA Password Remote Configuration – Principle of Operation

The sequence to remotely configure a MoCA® Password on a MoCA New Node through the coax medium could be implemented as follows:

1. Over the Pre-Admission Transport Service the management entity of the NC could perform an authentication protocol with the entity of the NN's device, that allows the management entity connected to the NC to uniquely identify a New Node's device prior to the node admission to the MoCA network.

   This device authentication protocol is vendor or service provider specific and agnostic to MoCA.

2. After the device has been successfully authenticated, the NC management entity could either:
   a. execute over the Pre-Admission Transport Service a vendor specific or proprietary protocol to create a secured channel and distribute the MoCA password(s) to the NN's management entity, as illustrated in Figure 1.

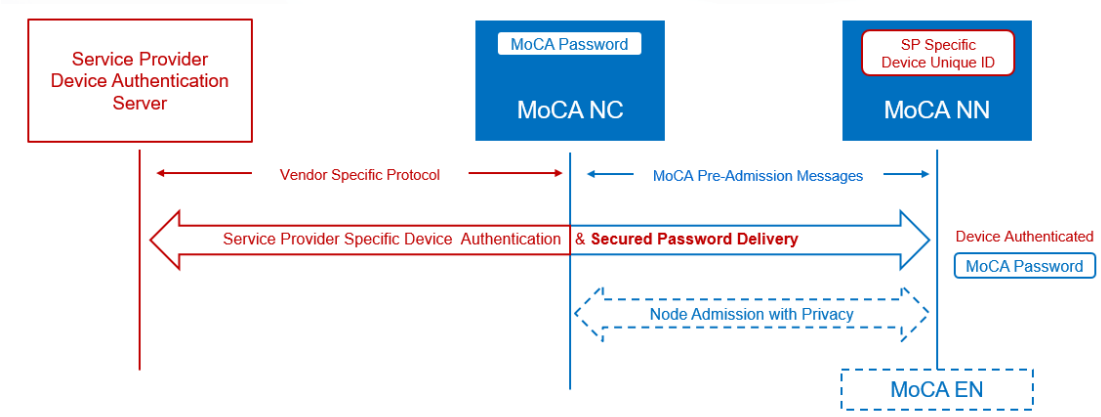

Figure 1. Device Authentication and Password Delivery through Service Provider Specific Protocol

   b. take advantage in MoCA 2.5 and MoCA3.0 of the native MoCA Protected Setup (MPS) (specified in their respective MoCA M/P specifications [2],[3]) to distribute the MoCA Password(s), as illustrated in Figure 2.

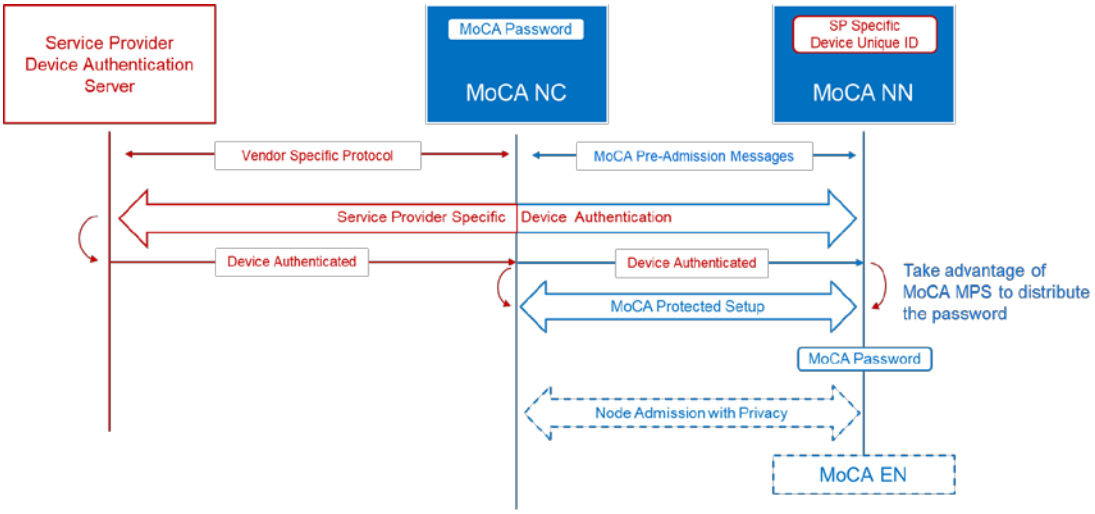

Figure 2. Device Authentication through Service Provider Specific Protocol and Password Delivery using MoCA® Protected Setup

7.1 *Example of Password Remote Configuration Message Handshake*

Figure 3 shows an example of message handshake that could take place over the Pre-Admission Transport Service containers to remotely configure the MoCA® Password(s) on a New Node:

Note: In the figure below the (red) messages are the Vendor Specific messages agnostically transported by the (blue) Pre-Admission Transport containers. The red arrows are the Vendor Specific protocol handling.

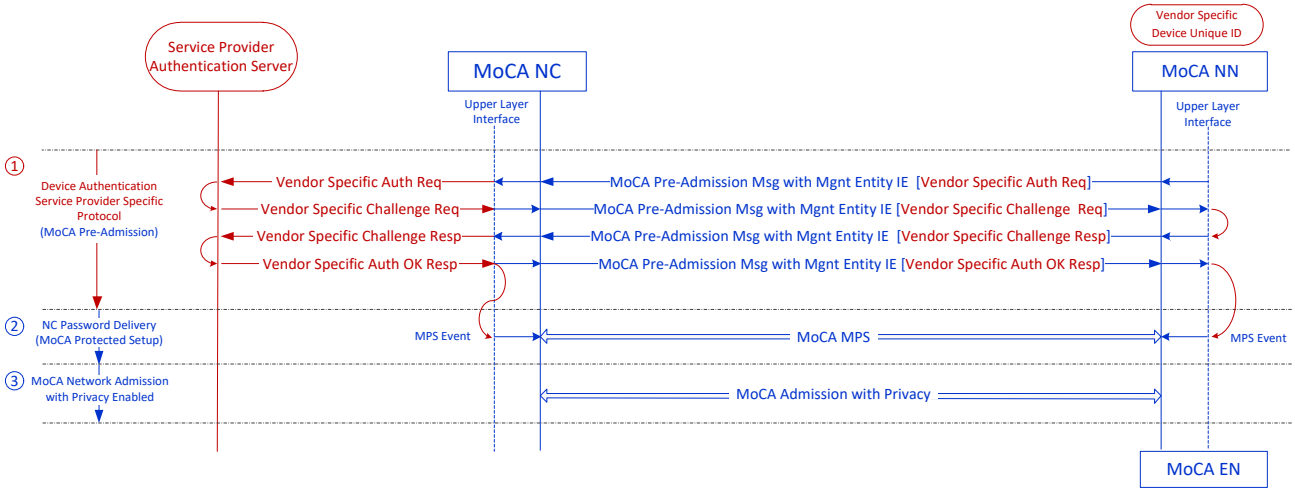

Figure 3. Example of Password Remote Configuration Message Handshake