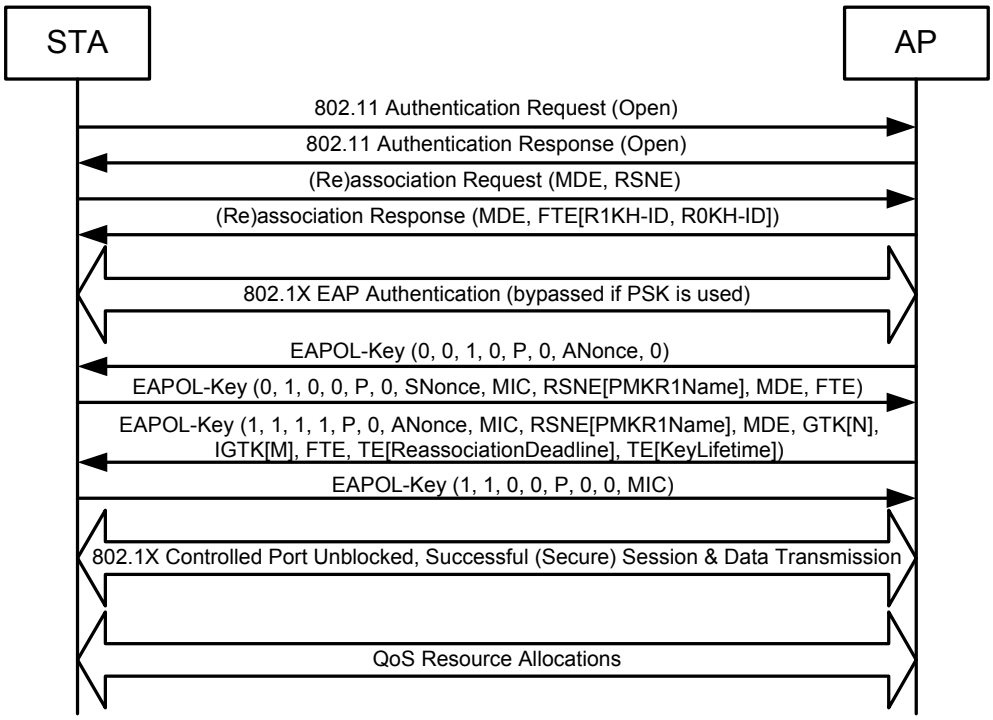

Figure 12-2—FT initial mobility domain association in an RSN

If the contents of the MDE received by the AP do not match the contents advertised in the Beacon and Probe Response frames, the AP shall reject the (Re)Association Request frame with status code 54 (i.e., Invalid MDE). If an MDE is present in the (Re)Association Request frame and the contents of the RSNE do not indicate a negotiated AKM of Fast BSS Transition (suite type 00-0F-AC:3, 00-0F-AC:4, or 00-0F-AC:9), the AP shall reject the (Re)Association Request frame with status code 43 (i.e., Invalid AKMP).

The (Re)Association Response frame from the AP shall contain an MDE, with contents as presented in Beacon and Probe Response frames. The FTE shall include the key holder identities of the AP, the R0KH-ID and R1KH-ID, set to the values of dot11FTR0KeyHolderID and dot11FTR1KeyHolderID, respectively. The FTE shall have a MIC element count of zero (i.e., no MIC present) and have ANonce, SNonce, and MIC fields set to 0.

On successful (re)association, the S0KH on the STA and the R0KH on the AP then proceed with an IEEE 802.1X authentication using EAPOL messages carried in IEEE 802.11 data frames if SAE authentication was not performed (i.e., if the suite type is not 00-0F-AC:9). The S0KH shall use the value of R0KH-ID as the endpoint identifier of the NAS Client (NAS-Identifier if RADIUS is used) in the exchange as defined in IETF RFC 3748-2004 [B38].

If IEEE 802.1X authentication was performed, then upon successful completion of authentication, the R0KH receives the MSK and authorization attributes. If SAE authentication was performed, the R0KH receives the PMK, resulting in the successful completion of SAE. If a key hierarchy already exists for this STA belonging to the same mobility domain (i.e., having the same MDID), the R0KH shall delete the existing PMK-R0 security association and PMK-R1 security associations. It then calculates the PMK-R0, PMKR0Name, and PMK-R1 and makes the PMK-R1 available to the R1KH of the AP with which the STA is associated.

If the SME of the STA cannot authenticate the AS, then it shall disassociate with an MLME-DISASSOCIATE.request primitive. If the AS signals the Authenticator that the STA cannot be

