TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 10176-8-12:2017
ISO/IEC 29341-8-12:2008

CÔNG NGHỆ THÔNG TIN - KIẾN TRÚC THIẾT BỊ UPNP - PHẦN 8-12: GIAO THỨC ĐIỀU KHIỂN THIẾT BỊ INTERNET GATEWAY - DỊCH VỤ XÁC THỰC LIÊN KẾT

Information technology - UPnP Device Architecture - Part 8-12: Internet Gateway Device Control Protocol - Link Authentication Service

HÀ NỘI - 2017

Mục lục **Trang**

Lời nói đầu

TCVN 10176-8-12:2017 hoàn toàn tương đương với ISO/IEC 29341-8-12:2008

TCVN 10176-8-12:2017 do Tiểu Ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC 1/SC 35 *Giao diện người sử dụng* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ TCVN 10176-8 *Công nghệ thông tin – Kiến trúc thiết bị UPnP* gồm các tiêu chuẩn sau:

- TCVN 10176-8-1:2017 (ISO/IEC 29341-8-1:2008), Phần 8-1: Giao thức điều khiển thiết bị internet gateway – Thiết bị internet gateway

- TCVN 10176-8-2:2017 (ISO/IEC 29341-8-2:2008), Phần 8-2: Giao thức điều khiển thiết bị internet gateway – Thiết bị mạng cục bộ

- TCVN 10176-8-3:2017 (ISO/IEC 29341-8-3:2008), Phần 8-3: Giao thức điều khiển thiết bị internet gateway – Thiết bị mạng diện rộng

- TCVN 10176-8-4:2017 (ISO/IEC 29341-8-4:2008), Phần 8-4: Giao thức điều khiển thiết bị internet gateway – Thiết bị kết nối mạng diện rộng

- TCVN 10176-8-5:2017 (ISO/IEC 29341-8-5:2008), Phần 8-5: Giao thức điều khiển thiết bị internet gateway – Thiết bị điểm truy cập mạng cục bộ không dây

- TCVN 10176-8-10:2017 (ISO/IEC 29341-8-10:2008), Phần 8-10: Giao thức điều khiển thiết bị internet gateway – Dịch vụ quản lý cấu hình host mạng cục bộ

- TCVN 10176-8-11:2017 (ISO/IEC 29341-8-11:2008), Phần 8-11: Giao thức điều khiển thiết bị internet gateway – Dịch vụ chuyển tiếp tầng 3

- TCVN 10176-8-12:2017 (ISO/IEC 29341-8-12:2008), Phần 8-12: Giao thức điều khiển thiết bị internet gateway – Dịch vụ xác thực liên kết

- TCVN 10176-8-13:2017 (ISO/IEC 29341-8-13:2008), Phần 8-13: Giao thức điều khiển thiết bị internet gateway – Dịch vụ radius từ máy trạm

Bộ tiêu chuẩn quốc tế ISO/IEC 29341-8 Information technology - *UPnP device architecture* còn các tiêu chuẩn sau:

- ISO/IEC 29341-8-14:2008, Part 8-14: Internet Gateway Device Control Protocol - Wide Area Network Cabre Link Configuration Service

- ISO/IEC 29341-8-15:2008, Part 8-15: Internet Gateway Device Control Protocol - Wide Area Network Common Interface Configuration Service

- ISO/IEC 29341-8-16:2008, Part 8-16: Internet Gateway Device Control Protocol - Wide Area Network Digital Subscriber Line Configuration Service

- ISO/IEC 29341-8-17:2008, Part 8-17: Internet Gateway Device Control Protocol - Wide Area Network Ethernet Link Configuration Service

- ISO/IEC 29341-8-18:2008, Part 8-18: Internet Gateway Device Control Protocol - Wide Area Network Internet Protocol Connection Service

- ISO/IEC 29341-8-19:2008, Part 8-19: Internet Gateway Device Control Protocol - Wide Area Network Plain Old Telephone Service Link Configuration Service

- ISO/IEC 29341-8-20:2008, Part 8-20: Internet Gateway Device Control Protocol - Wide Area Network Point-to-Point Protocol Connection Service

- ISO/IEC 29341-8-21:2008, Part 8-21: Internet Gateway Device Control Protocol - Wireless Local Area Network Configuration Service

Công nghệ thông tin - Kiến trúc thiết bị UPnP - Phần 8-12: Giao thức điều khiển thiết bị internet gateway - Dịch vụ xác thực liên kết

Information technology – UPnP device architecture – Part 8-12: Internet gateway device control protocol – Link authentication service

1 Phạm vi áp dụng

Tiêu chuẩn này phù hợp với kiến trúc thiết bị UPnP, phiên bản 1.0.

Kiểu dịch vụ này cho phép điểm điều khiển UPnP tạo cấu hình và điều khiển các thông số liên quan đến việc xác thực bởi máy chủ xác thực. Dịch vụ này quy định các biến và các hoạt động được sử dụng bởi các điểm điều khiển để thêm, cập nhật và xóa các bản ghi sử dụng để xác thực. Việc này được sử dụng để duy trì các thông số xác thực trên thiết bị theo từng máy trạm. Dịch vụ này hỗ trợ danh mục người sử dụng/ khách với các chứng thực (mật khẩu, khóa công khai) và các quyền truy cập cụ thể trên cơ sở mỗi người sử dụng. Dịch vụ được thiết kế chính cho việc xác thực trên điểm truy cập không dây tại đó thực thi an ninh tầng liên kết như là chuẩn 802.1x. Ngoài ra còn được sử dụng nhằm các mục đích khác – ví dụ: lưu trữ một cách an toàn các chứng thực máy trạm ví dụ các chứng chỉ và các khóa phi đối xứng cho các giao thức an ninh tầng mạng.

Tuy nhiên, Ban working committee chỉ xem xét dịch vụ này từ khía cạnh sử dụng chuẩn 802.1x, do đó tiêu chuẩn này đưa ra một vài tham chiếu đến giao thức theo chuẩn 802.1x. Dịch vụ này có thể đặt cùng chỗ với thiết bị điểm truy cập mà yêu cầu dịch vụ xác thực hoặc định vị trên thiết bị khác nhau trong mạng như là thiết bị internet gateway. Dịch vụ này được xác định nhằm kết hợp máy trạm WLAN và chứng thực của chúng để tự khởi động WLAN an toàn trong công nghệ UPnP tương thích với *WLANAccessPointDevice*[*]

Dịch vụ này được xác định là dịch vụ thành phần độc lập. Mọi sản phẩm thực thi đặc tả thiết bị chuẩn sẽ có lựa chọn để thực thi đặc tả dịch vụ này. Tại thời điểm kiểm thử chứng nhận, sản phẩm sẽ được kiểm thử cho dịch vụ này ngoài việc được kiểm thử cho kiểu thiết bị gốc của sản phẩm (ví dụ: *WLANAccessPointDevice, InternetGatewayDevice*)

---

[*] Tham khảo các tài liệu kèm theo xác định bởi Ban UPnP internet gateway working committee để biết thêm chi tiết về các thiết bị và dịch vụ cụ thể tham chiếu trong tiêu chuẩn này.

2 Xác định mô hình dịch vụ

2.1 Kiểu dịch vụ

Kiểu dịch vụ sau đây định danh dịch vụ phù hợp với mẫu này:

urn:schemas-upnp-org:sevice:*LinkAuthentication:1*

2.2 Các biến trạng thái

Bảng 1 - Các biến trạng thái

Tên biến	Bắt buộc hoặc tùy chọn	Kiểu dữ liệu	Giá trị cho phép[1]	Giá trị mặc định[1]	Đơn vị
NumberOfEntries	Bắt buộc	Ui2	>=0	0	Không xác định
Identifier	Bắt buộc	String	<=64 ký tự	Chuỗi rỗng	Không xác định
Secret	Bắt buộc	String	Mã hóa trong BASE64, <=1024 ký tự	Chuỗi rỗng	Không xác định
SecretType	Bắt buộc	String	Xem Bảng 1.1, <=32 ký tự	Không quy định	Không xác định
AuthType	Bắt buộc	String	Xem Bảng 1.2, <=32 ký tự	Không quy định	Không xác định
AuthState	Bắt buộc	String	Xem Bảng 1.3, <=32 ký tự	Không có cấu hình	Không xác định
CredentialState	Bắt buộc	String	Xem Bảng 1.4, <=32 ký tự	Không có cấu hình	Không xác định
Description	Bắt buộc	String	<= 256 ký tự	Chuỗi rỗng	Không xác định
MACAddress	Bắt buộc	String	Địa chỉ MAC, "xx:xx:xx:xx:xx:xx, ", không phụ thuộc loại chữ, 17 ký tự	Chuỗi rỗng	Không xác định
CredentialDuration	Bắt buộc	Ui4	>=0	0	Giây
LinkIdentifier	Bắt buộc	String	<=64 ký tự	Chuỗi rỗng	Không xác định
LastChange	Bắt buộc	String	<=1024 ký tự	Chuỗi rỗng	Không xác định
LastError	Bắt buộc	String	<=1024 ký tự	Chuỗi rỗng	Không xác định
Các biến trạng thái không theo chuẩn do nhà cung cấp cài đặt	Không theo chuẩn	Chưa xác định	Chưa xác định	Chưa xác định	Chưa xác định

[1] các giá trị liệt kê trong cột này là yêu cầu. Để quy định các giá trị tùy chọn chuẩn hoặc để ủy quyền việc ấn định các giá trị cho nhà cung cấp, bạn phải tham chiếu thể hiện cụ thể của bảng thích hợp dưới đây

2.2.1 NumberOfEntries

Biến này cho biết số lượng các mục nhập trong cơ sở dữ liệu xác thực.

2.2.2 Identifier

Biến này tương tự với trường tên người sử dụng hoặc trường định danh người sử dụng. Trường này được đối sánh khi người sử dụng cung cấp chuỗi định danh EAP (extensible authentication protocol- giao thức xác thực mở rộng). Dịch vụ này giả định là bộ định danh định danh duy nhất mỗi bản ghi trong cơ sở dữ liệu xác thực, nghĩa là không có bản ghi nào có các trường định danh trùng lặp. Chú ý, EAP sử dụng thuật ngữ Identifier để tham chiếu đến octet (bộ tám) đơn nhằm đối sánh yêu cầu và các phản hồi EAP, trong đặc tả này, trường Identifier tham chiếu đến chuỗi định danh EAP. Xem RFC 2716 điều 3.1. Bộ định danh có thể chứa các ký tự < > & trong đó sẽ "phá vỡ" các dòng XML bao quanh, do đó, chuỗi định danh phải được đánh dấu 'escaped'. Tham khảo phần thiết bị "Các chuỗi XML là các thông số UPnP"

2.2.3 Secret

Biến này chứa trường Secret cho từng kiểu quy định trong trường `SecretType`. Nó được mã hóa như chuỗi trong BASE64 chính tắc (được sử dụng bởi dịch vụ an ninh thiết bị)

2.2.4 SecretType

Biến này quy định kiểu secret chứa trong trường `secret`. Các giá trị của chuỗi có thể xảy ra được quy định trong bảng 1.1.

Bảng 1.1- Danh mục giá trị cho phép cho `SecretType`

Giá trị	Bắt buộc hoặc tùy chọn	Mô tả
TextPassword	Bắt buộc	Giá trị này cho biết trường `Secret` chứa mật khẩu dạng văn bản
X509Certificate	Bắt buộc	Giá trị này cho biết trường `Secret` chứa chứng thực X.509
PublicKey	Bắt buộc	Giá trị này cho biết trường `Secret` chứa khóa công khai
PubKeyHash160	Bắt buộc	Giá trị này cho biết trường `Secret` chứa hàm băm 160 bit của khóa công khai
Vendor-defined	Bắt buộc	Bắt buộc
Vendor-defined	Bắt buộc	Tùy chọn

2.2.5 AuthType

Biến này quy định kiểu xác thực. Các giá trị chuỗi có thể xảy ra được quy định trong bảng 1.2.

Bảng 1.2- Danh mục giá trị cho phép cho `AuthType`

Giá trị	Bắt buộc hoặc tùy chọn	Mô tả
SharedSecret	Bắt buộc	Giá trị này cho biết chuẩn máy trạm 802.1x sử dụng phương pháp xác thực trong đó yêu cầu thêm một chứng thực như là bí mật chia sẻ đang khuyết, ví dụ `TextPassword`. Khi kiểu xác thực là `Pending` thì người sử dụng được giả định cung cấp bí mật chia sẻ cho AP thông qua điểm điều khiển sử dụng hoạt động `UpdateEntry`. Điều này dẫn đến một thay đổi trong giá trị trường `Secret`.
ValidateCredentials	Bắt buộc	Giá trị này cho biết chuẩn máy trạm 802.1x đang sử dụng phương pháp xác thực trong đó yêu cầu xác minh các chứng thực hiện có, tức là như trong chứng thực X509. Khi `AuthState` là `pending` thì điều này yêu cầu người sử dụng hoặc điểm điều khiển xác nhận tính hợp lệ của chứng thực trong trường `Secret`
Vendor-defined		Bắt buộc
Vendor-defined	Tùy chọn	Tùy chọn

2.2.6 AuthState

Biến này quy định trạng thái hiện hành của quá trình xác thực. Các giá trị chuỗi có thể xảy ra được quy định trong bảng 1.3. Tham khảo biểu đồ trạng thái và lý thuyết vận hành để biết thêm chi tiết.

Bảng 1.3- Danh mục giá trị cho phép cho `AuthType`

Giá trị	Bắt buộc hoặc tùy chọn	Mô tả
Unconfigured	Bắt buộc	Máy trạm WLAN tương ứng với biến `Identifier` cần phải xác thực.
Failed	Bắt buộc	Máy trạm WLAN tương ứng với biến `Identifier` xác thực không thành công các nội dung của trường `secret` – ví dụ, với xác thực theo chuẩn 802.1x. Trạng thái này thông báo với các điểm điều khiển bí mật đã được nhập hoặc xác nhận tính hợp lệ thất bại.
Succeed	Bắt buộc	Máy trạm WLAN đương ứng với biến `Identifier` xác thực thành công các nội dung của trường `secret` – ví dụ, với xác thực theo chuẩn 802.1x. Trạng thái này thông báo với các điểm điều khiển bí mật mà được nhập hoặc xác nhận tính hợp lệ thành công.
Vendor-defined	Bắt buộc	Bắt buộc
Vendor-defined	Tùy chọn	Tùy chọn

2.2.7 CredentialState

Biến này quy định trạng thái hiện hành của quá trình phê duyệt/xác nhận tính hợp lệ của chứng thực. Các giá trị chuỗi có thể xảy ra được quy định trong bảng 1.4. Tham khảo biểu đồ trạng thái và lý thuyết vận hành để biết thêm chi tiết.

Bảng 1.4 - Danh mục giá trị cho phép cho `CredentialState`

Giá trị	Bắt buộc hoặc tùy chọn	Mô tả
Unconfigured	Bắt buộc	Giá trị này cho biết rằng các biến khác trong bản ghi nào đó không được khởi tạo hoặc trong trạng thái không hợp lệ. Các ví dụ về các biến này bao gồm `Secret` và `AuthType`. Bản ghi này sẽ không được sử dụng cho việc xác thực, nó có thể được sử dụng cho các mục đích khác.
Pending (CP báo động cho hoạt động)	Bắt buộc	Giá trị này cho biết bản ghi được tham chiếu đến trường `Identifier` không có trường `Secret` hợp lệ. Các điểm điều khiển được kỳ vọng nhắc nhở người sử dụng cuối nhập giá trị SharedSecret hoặc xác nhận tính hợp lệ của một chứng thực. Nhờ vào việc chấp nhận người sử dụng cuối, điểm điều khiển thay đổi biến `AuthState` thành `Accepted` hoặc `Denied`.
Accepted	Bắt buộc	Giá trị này cho biết bản ghi cơ sở dữ liệu tham chiếu đến trường `Identifier` có trường `Secret` đã được nhập/xác nhận tính hợp lệ bởi người sử dụng cuối.
Denied	Bắt buộc	Giá trị này cho biết rằng khi máy trạm cố gắng xác thực, nhưng không được phép tiếp tục với xác thực tầng liên kết. Trạng thái này nhằm mục đích giới hạn các thiết bị từ mạng và giới hạn các sự kiện từ các thiết bị khác.
Vendor-defined	Bắt buộc	Bắt buộc
Vendor-defined	Tùy chọn	Tùy chọn

Thành phần thực hiện việc xác thực và cấp quyền truy cập mạng được kỳ vọng tham chiếu tới cơ sở dữ liệu của máy trạm đối với thông tin chứng thực. Nếu trường `Identifier` cho trước không được tìm thấy trong cơ sở dữ liệu thì một bản ghi mới sẽ được thiết lập, điền và thiết lập là Pending. Thông qua điểm điều khiển, người sử dụng có thể cập nhật bản ghi là `Accepted` hoặc `Denied`. Điểm điều khiển có thể truy vấn người sử dụng về tổng số thời gian cấp máy trạm truy cập mạng tạm thời. Tổng số thời gian được quy định tính bằng giây và được lưu trữ trong biến `CredentialDuration`.

2.2.8 Description

Biến này lưu trữ một chuỗi được sử dụng độc quyền bởi các điểm điều khiển nhằm giúp việc định danh các bản ghi xác thực. Ví dụ, điểm điều khiển có thể nhắc người sử dụng cung cấp tên thân thiện với thiết bị máy trạm. Nó được lưu trữ trong các bản ghi xác thực và không thể được sử dụng bởi thiết bị AP. Biến Description có thể chứa các ký tự < > $ sẽ "phá vỡ" các dòng XML bao quanh, đo đó, chuỗi Description phải được đánh dấu 'escaped'. Tham khảo An ninh thiết bị phần "Các chuỗi XML là các thông số UPnP"

2.2.9 MACAddress

Biến này quy định địa chỉ MAC (Media Access Control – kiểm soát truy cập môi trường) của máy trạm. Biến này không được sử dụng để xác thực máy trạm, khi địa chỉ MAC có thể thay đổi. Trường này có thể được sử dụng bởi các điểm điều khiển để biểu diễn địa chỉ MAC của thiết bị trong suốt quá trình xác thực ban đầu khi thiết bị máy trạm ban đầu được thêm vào mạng và cơ sở dữ liệu xác thực. Trường này cũng được cập nhật để phản ánh địa chỉ MAC cuối cùng được xác thực thành công hoặc không thành công. Xem điều 2.3 để biết thêm chi tiết.

2.2.10 CredentialDuration

Biến này định rõ thời điểm (theo số giây) một bản ghi của máy trạm với trường `CredentialState` của giá trị `Accepted` được phép xác thực. Giá trị 0 có nghĩa là bản ghi của máy trạm là không đổi, sẽ không xảy ra trường hợp hết hiệu lực. Các giá trị khác không quy định truy cập tạm thời. Khi sự chuyển tiếp trường `CredentialDuration` khác 0 thành giá trị 0 (số giây hết hiệu lực) thì bản ghi phải bị xóa và sự kiện LastChange được kích khởi. Chú ý rằng các bản ghi của máy trạm không đổi với trường `CredentialDuration` có giá trị 0 vẫn tiếp tục cài đặt hoặc khởi động lại thiết bị. Tùy thuộc vào các nhà cung cấp để thực thi tính biến bỉ khi thích hợp cho thiết bị của họ, ví dụ lưu trữ trong bộ nhớ không thay đổi được như là flash hoặc disk. Các giá trị của trường `CredentialDuration` khác 0 sẽ không tiếp tục cài đặt hoặc khởi động lại thiết bị, máy trạm tạm thời giả định được xác thực lại. Số giây còn lại có thể được trích xuất qua các hoạt động `GetGenericEntry` và `GetSpecificEntry`. Sự giảm bớt số giây tự động cho trường `CredentialDurationc` không phát sinh sự kiện `LastChange`.

2.2.11 LinkedIdentifier

Một vài phương pháp xác thực cho phép hai thỏa thuận EAP. Ví dụ, PEAP (Protectd-EAP) thỏa thuận hai giai đoạn, đó là phần 1 và phần 2 nhằm hoàn thiện việc xác thực. Mỗi giai đoạn có thể thỏa thuận sử dụng các bộ định danh duy nhất, các kiểu xác thực và các chứng thực. Để cho phép máy chủ EAP chỉ ra các bản ghi liên quan cho điểm điều khiển thì trường này chứa định danh cho sự phủ nhận EAP ban đầu. Ví dụ, nếu PEAP phần 1 sử dụng trong bộ định danh của người sử dụng 1, kiểu xác thực `ValidateCredentials`, kiểu bí mật PubKeyHash160 và PEAP phần 2 sử dụng bộ định danh của người sử dụng 2, kiểu xác thực SharedSecret, thì hai bản ghi sẽ tồn tại với trường LinkedIdentifier của bản ghi người sử dụng 2 chứa người sử dụng 1. Do đó,

nếu giai đoạn xác thực phần 2 thất bại thì máy chủ EAP nên xóa cả hai bản ghi người sử dụng 1 và người sử dụng 2. Ngoài ra, nếu người sử dụng từ chối xác thực phần 2 thì điểm điều khiển sẽ thiết lập cả hai bản ghi CredentialState là Denied hoặc xóa tùy chọn cả hai bản ghi người sử dụng 1 và người sử dụng 2.

Biến LinkedIndentifier có thể chứa các ký tự < > $ sẽ "phá vỡ" dòng XML bao quanh, đo đó, chuỗi Description phải được đánh dấu 'escaped'. Tham khảo An ninh thiết bị phần "Các chuỗi XML là các thông số UPnP"

2.2.12 LastChange

Biến này được sử dụng cho các mục đích ghi lại sự kiện, cho phép các điểm điều khiển trích xuất các thông báo có nghĩa về sự kiện khi bản ghi được thêm, được xóa hoặc được thay đổi.

`LastChange` là một biến chuỗi được ghi lại sự kiện mà giá trị của nó là chuỗi XML đã thoát (được sử dụng bởi dịch vụ an ninh thiết bị) với định dạng sau đây (khoảng trống trắng được trình bày có thể đọc được nhưng không cần thiết):

```
<action>
        <fieldname>value</fieldname>...
</action>
```

Trong đó, `action` là một trong các giá trị sau {`Add`, `Delete`, `Update`}, `fieldname` là một trong các giá trị sau {`Indentifier`, `Secret`, `SecretType`, `AuthType`, `AuthState`, `CredentialState`, `LinkedIdentifier`} và `value` được quy định cho mỗi bảng của các biến trạng thái. Biến `Indentifier` phải luôn có mặt. Để ngăn việc gửi biến `Secret` (có thể là chuỗi lớn) qua mạng thì chuỗi rỗng nên được gửi tại vị trí của nó. Điều này nhằm mục đích giảm bớt lưu lượng sự kiện `LastChange` kích khởi và cũng tránh việc gửi thông tin nhạy cảm qua các thông điệp sự kiện. Nhiều thay đổi cho bản ghi đơn có thể được móc nối vào nhau nhằm kích khởi sự kiện đơn cho các điểm điều khiển đã đăng ký. Khi bản ghi được cập nhật thì sẽ có khuyến cáo rằng chỉ có các trường trong đó giá trị của chúng thay đổi được gửi đi nhưng điều này không giả định với các điểm điều khiển.

Ví dụ, việc tạo bản ghi mới có thể dẫn đến giá trị cho biến `LastChange` sau đây:

```
<Add>
      <Identifier>Foo</Identifier>
      <Secret/>
      <SecretType>TextPassword</SecretType>
      <AuthType>SharedSecret</AuthType>
      <AuthState>Unconfigured</AuthState>
      <CredentialState>Unconfigured</CredentialState>
</Add>
```

Thay đổi tiếp theo cho CredentialState có thể dẫn đến giá trị sau đây:

```
<Update>
    <Identifier>Foo</Identifier>
    <CredentialState>Pending</CredentialState>
</Update>
```

2.2.13 LastError

Biến này nhằm mục đích ghi lại sự kiện nhằm cho phép các điểm điều khiển phát hiện khi một lỗi không đồng bộ (nghĩa là lỗi mà không phải kết quả trực tiếp của hoạt động UPnP) xảy ra trong bộ xử lý nền của máy chủ xác thực. Ví dụ, máy chủ EAP cố gắng thêm một bản ghi mới cho cơ sở dữ liệu xác thực nhưng không thực hiện được do thiếu tài nguyên.

Biến `LastError` là một biến chuỗi được ghi lại sự kiện mà giá trị của nó là chuỗi XML đã thoát (được sử dụng bởi dịch vụ an ninh thiết bị)với định dạng sau đây (khoảng trống trắng được trình bày có thể đọc được nhưng không cần thiết)

```
<Error>
    <Code>integer-code</Code>
    <Description>error-description</Description>
</Error>
```

Khi thích hợp, các mã lỗi UPnP và các mô tả có thể được sử dụng. Các mã mới nên được phân bố theo các quy ước mô tả trong điều 2.4.9.

2.3 Ghi lại sự kiện và kiểm duyệt.

Bảng 2 - Kiểm duyệt sự kiện

Tên biến	Ghi lại sự kiện	Sự kiện kiểm duyệt	Tỉ lệ sự kiện tối đa[1]	Liên kết logic	Delta tối thiểu cho mỗi sự kiện[2]
`LastChange`	Có	Không	Không xác định	Không xác định	Không xác định
`LastError`	Có	Không	Không xác định	Không xác định	Không xác định
Các biến trạng thái không theo chuẩn do nhà cung cấp UPnP cài đặt	*Chưa xác định*	*Chưa xác định*	*Chưa xác định*	*Chưa xác định*	*Chưa xác định*

[1]Được xác định bởi N, trong đó Tỉ lệ =(Sự kiện)/(N giây)
[2](N)*(Bước khoảng giá trị cho phép)

2.3.1 Mô hình sự kiện

Các điểm điều khiển có thể sử dụng các sự kiện của biến `LastChange` để thông báo cho người dùng cuối việc máy trạm cố gắng truy cập mạng thời điểm đầu tiên và có thể sử dụng các sự kiện của biến `LastError` để thông báo các lỗi không đồng bộ. Ngoài ra, các điểm điều khiển có thể

sử dụng các sự kiện để nhân đôi hoặc sao chép dự phòng cơ sở dữ liệu xác thực cho điểm điều khiển như là PC hoặc bên trong điểm truy cập không dây khác. Tham khảo điều 2.3 để biết thêm chi tiết.

CHÚ THÍCH: Các sự kiện độc lập không thể được sử dụng để nhân đôi cơ sở dữ liệu bởi vì chúng sẽ không chứa giá trị của trường `Secret`. Điểm điều khiển có thể sử dụng hoạt động `GetSpecificEntry` để trích xuất giá trị của nó.

2.4 Các hoạt động

Bảng 3 liệt kê các hoạt động bắt buộc hoặc tùy chọn cho thiết bị UPnP. Tiếp theo đó là thông tin chi tiết về các hoạt động này, bao gồm các mô tả ngắn về các hoạt động, các kết quả của hoạt động trên các biến trạng thái và các mã lỗi xác định bởi các hoạt động.

Các hoạt động UPnP an toàn trong dịch vụ này được khuyến cáo là tùy chọn, sử dụng các giao thức an ninh UPnP như được xác định bởi nhóm công tác an ninh UPnP. Nếu AP thực thi an ninh cho các hoạt động của UPnP thì Bảng 3 sẽ cho biết các hoạt động là an toàn. Các AP còn lại có thể được thực thi là an toàn hoặc mở. Các hoạt động an toàn phải được bảo vệ cả về tính cẩn mật lẫn tính toàn vẹn.

Các quyền truy cập sẽ được kế thừa từ thiết bị chứa (ví dụ: thiết bị điểm truy cập WLAN)

Bảng 3 - Các hoạt động

Tên	An toàn hoặc Mở*	Bắt buộc hoặc tùy chọn
`GetGenericEntry`	An toàn	Bắt buộc
`GetSpecificEntry`	An toàn	Bắt buộc
`AddEntry`	An toàn	Bắt buộc
`UpdateEntry`	An toàn	Bắt buộc
`DeleteEntry`	An toàn	Bắt buộc
`GetNumberOfEntries`	An toàn	Bắt buộc
`FactoryDefaultReset`	An toàn	Bắt buộc
`ResetAuthentication`	An toàn	Bắt buộc
Các hoạt động không theo chuẩn do nhà cung cấp UPnP cài đặt		*Không theo chuẩn*
* Cột này thích hợp nếu dịch vụ an ninh thiết bị có mặt trong thiết bị bộ chứa		

2.4.1 GetGenericEntry

Hoạt động này trích xuất một mục nhập của các bản ghi xác thực tại một thời điểm. Các điểm điều khiển có thể gọi hoạt động này với chỉ mục mảng tăng cho đến khi có nhiều mục hơn được tìm thấy trong danh mục bản ghi xác thực. Nếu biến LastChange được cập nhật trong suốt cuộc gọi thì thì quá trình phải bắt đầu lại. Các mục nhập trong mảng là liền nhau. Khi các mục nhập bị xóa thì mảng được kết lại thành khối và biến sự kiện LastChange được kích khởi. Các bản ghi

xác thực được lưu trữ logic như một mảng và được trích xuất bằng cách sử dụng chỉ mục mảng sắp xếp có thứ tự từ 0 đến NumberOfEntries-1.

2.4.1.1 Các đối số

Bảng 4- Các đối số cho `GetGenericEntry`

Đối số	Hướng	Biến trạng thái liên quan
NewIndex	IN	NumberOfEntries
NewIdentifier	OUT	Identifier
NewSecret	OUT	Secret
NewSecretType	OUT	SecretType
NewAuthType	OUT	AuthType
NewAuthState	OUT	AuthState
NewCredentialState	OUT	CredentialState
NewDescription	OUT	Description
NewMACAddress	OUT	MACAddress
NewCredentialDuration	OUT	CredentialDuration
NewLinkedIdentifier	OUT	LinkedIdentifier

2.4.1.2 Phụ thuộc vào trạng thái (nếu có)

2.4.1.3 Ảnh hưởng đến trạng thái (nếu có)

Không có thông tin

2.4.1.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem kiến trúc thiết bị UPnP phần Điều khiển
713	Chỉ mục mảng đã quy định không hợp lệ	Chỉ mục mảng không thuộc phạm vi quy định

2.4.2 GetSpecificEntry

Hoạt động này trích xuất một mục nhập bản ghi xác thức được quy định bởi thông số đầu vào `NewIdentifierKey`. Các bản ghi xác thực được lưu trữ như một mảng trong danh mục bản ghi xác thực và có thể được trích xuất bằng cách sử dụng bộ định danh như một giá trị duy nhất.

2.4.2.1 Các đối số

Hình 5- Các đối số cho `GetSpecificEntry`

Đối số	Hướng	Biến trạng thái liên quan
`NewIdentifierKey`	IN	`IdentifierKey`
`NewIdentifier`	OUT	`Identifier`
`NewSecret`	OUT	`Secret`
`NewSecretType`	OUT	`SecretType`
`NewAuthType`	OUT	`AuthType`
`NewAuthState`	OUT	`AuthState`
`NewCredentialState`	OUT	`CredentialState`
`NewDescription`	OUT	`Discription`
`NewMACAddress`	OUT	`MACAddress`
`NewCredentialDuration`	OUT	`CredentialDuration`
`NewLinkedIdentifier`	OUT	`LinkedIdentifier`

2.4.2.2 Phụ thuộc vào trạng thái (nếu có)

2.4.2.3 Ảnh hưởng đến trạng thái

Không có thông tin

2.4.2.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem kiến trúc thiết bị UPnP phần Điều khiển
605	Đối số chuỗi quá dài	Đối số chuỗi quá dài để thiết bị vận hành chính xác
702	Không có mặt khóa định danh	Bản ghi tương ứng với khóa định danh đầu vào không được tìm thấy trong danh mục bản ghi xác thực.

2.4.3 AddEntry

Hoạt động này tạo một bản ghi xác thực mới

2.4.3.1 Các đối số

Bảng 6- Các đối số cho AddEntry

Đối số	Hướng	Biến trạng thái liên quan
NewIdentifier	IN	Identifier
NewSecret	IN	Secret
NewSecretType	IN	SecretType
NewAuthType	IN	AuthType
NewAuthState	IN	AuthState
NewCredentialState	IN	CredentialState
NewDescription	IN	Discription
NewMACAddress	IN	MACAddress
NewCredentialDuration	IN	CredentialDuration
NewLinkedIdentifier	IN	LinkedIdentifier
NewNumberOfEntries	OUT	NumberOfEntries

2.4.3.2 Phụ thuộc vào trạng thái (nếu có)

2.4.3.3 Ảnh hưởng đến trạng thái

Khi thêm một bản ghi mới thì biến LastChange được ghi lại sự kiện bao gồm trường và giá trị mới.

2.4.3.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem Kiến trúc thiết bị UPnP phần Điều khiển
501	Hoạt động thất bại	Xem Kiến trúc thiết bị UPnP phần Điều khiển
605	Đối số chuỗi quá dài	Đối số chuỗi quá dài để thiết bị vận hành chính xác
701	Có mặt mục nhập	Nếu bảo ghi hiện có với bộ định danh tồn tại trong cơ sở dữ liệu thì lỗi này sẽ được trả về.

2.4.4 UpdateEntry

Hoạt động này sử đổi một bản ghi xác thực hiện có.

2.4.4.1 Đối số

Bảng 7 - Đối số cho `UpdateEntry`

Đối số	Hướng	Biến trạng thái liên quan
`NewIdentifier`	IN	`Identifier`
`NewSecret`	IN	`Secret`
`NewSecretType`	IN	`SecretType`
`NewAuthType`	IN	`AuthType`
`NewAuthState`	IN	`AuthState`
`NewCredentialState`	IN	`CredentialState`
`NewDescription`	IN	`Discription`
`NewMACAddress`	IN	`MACAddress`
`NewCredentialDuration`	IN	`CredentialDuration`
`NewLinkedIdentifier`	IN	`LinkedIdentifier`
`NewNumberOfEntries`	OUT	`NumberOfEntries`

2.4.4.2 Phụ thuộc vào trạng thái (nếu có)

2.4.4.3 Ảnh hưởng đến trạng thái

Các trường và giá trị sửa đổi này được ghi lại sự kiện thông qua sự kiện `LastChange`.

2.4.4.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem Kiến trúc thiết bị UPnP phần Điều khiển
501	Hoạt động thất bại	Xem Kiến trúc thiết bị UPnP phần Điều khiển
605	Đối số chuỗi quá dài	Đối số chuỗi quá dài để thiết bị vận hành chính xác
714	Không có mặt mục nhập	Nếu tồn tại bản ghi hiện có với bộ định danh thì lỗi này sẽ được trả về.

2.4.5 DeleteEntry

Hoạt động này xóa bản ghi xác thực quy định bởi bộ định danh.

2.4.5.1 Các đối số

Bảng 8 - Các đối số đối với `DeleteEntry`

Đối số	Hướng	Biến trạng thái liên quan
`NewIdentifier`	IN	`Identifier`
`NewNumberOfEntries`	OUT	`NumberOfEntries`

2.4.5.2 Phụ thuộc vào trạng thái (nếu có)

2.4.5.3 Ảnh hưởng đến trạng thái

Khi mỗi mục nhập bị xóa thì mảng sẽ được kết lại thành khối và biến sự kiện `LastChange` được kích khởi. Biến `LastChange` bao gồm trường hoạt động đặt là Delete được theo sau bởi trường `Identifier`.

2.4.5.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem Kiến trúc thiết bị UPnP phần Điều khiển
605	Đối số chuỗi quá dài	Đối số chuỗi quá dài để thiết bị vận hành chính xác
702	Không có mặt khóa định danh	Bản ghi tương ứng với khóa định danh đầu vào không được tìm thấy trong danh mục bản ghi xác thực.

2.4.6 GetNumberOfEntries

Hoạt động này trích xuất giá trị `NumberOfEntries`.

2.4.6.1 Các đối số

Bảng 9 - Các đối số cho `GetNumberOfEntries`

Đối số	*Hướng*	Biến trạng thái liên quan
`NewNumberOfEntries`	OUT	`NumberOfEntries`

2.4.6.2 Phụ thuộc vào trạng thái (nếu có)

2.4.6.3 Ảnh hưởng đến trạng thái (nếu có)

2.4.6.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem kiến trúc thiết bị UPnP phần Điều khiển

2.4.7 FactoryDefaultReset

Hoạt động này thiết lập lại dịch vụ cho các mặc định của hãng. Khi thực hiện thành công thì cơ sở dữ liệu xác thực sẽ chỉ chứa các mục nhập mà được nhà cung cấp xác định trước, nếu có.

Khuyến cáo rằng các sự kiện `LastChange` liên quan được đăng khi thiết lập lại các mặc định của hãng.

Tất cả các phiên xác thực sử dụng các chứng thực trong bộ nhớ phải được tách khỏi nhau.

Khi một thiết bị chứa có hoạt động FactoryDefaultReset của an ninh thiết bị được gọi thì hoạt động FactoryDefaultReset được xử lý bởi dịch vụ xác thực liên kết. Ngoài ra, nhóm công tác IGD định rõ rằng dịch vụ xác thực liên kết là dịch vụ con của dịch vụ cấu hình WLAN khi chứa trong thiết bị điểm truy cập WLAN. Do đó, khi hoạt động FactoryDefaultReset của dịch vụ cấu hình WLAN được gọi thì thực thi hoạt động FactoryDefaultReset của dịch vụ cấu hình WLAN phải gọi thực thi hoạt động FactoryDefaultReset của dịch vụ xác thực liên kết.

2.4.7.1 Các đối số

Không có thông tin.

2.4.7.2 Phụ thuộc vào trạng thái (nếu có)

2.4.7.3 Ảnh hưởng đến trạng thái

Không có thông tin, ngoài trừ thực tế là có thể nhận được bộ định tuyến khác.

2.4.7.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem kiến trúc thiết bị UPnP phần Điều khiển
501	Hoạt động thất bại	Xem Kiến trúc thiết bị UPnP phần Điều khiển

2.4.8 ResetAuthentication

Hoạt động này thực hiện một thiết lập mềm của dịch vụ. Điều này bắt buộc tất cả các máy trạm xác thực lại và bảo đảm rằng các biến `CredentialState` và `AuthState` là không đổi.

- Tất cả các phiên xác thực sử dụng các chứng thực trong bộ nhớ phải được tách khỏi nhau.

- Tất cả các mục nhập cơ sở dữ liệu xác thực tạm thời (tức là có các trường `CredentialDuration` khác 0) bị xóa.

- Tất cả các mục nhập với trường `CredentialState` khác với trường `Accepted` (các biến secret của chúng không bao giờ được xác nhận tính hợp lệ) bị xóa.

- Trường `AuthState` được đặt là `Unconfigured` đối với tất cả các mục nhập còn lại và máy chủ EAP tiếp tục với việc xác thực lại.

Yêu cầu rằng các sự kiện `LastChange` liên quan được đăng khi thực hiện thiết lập mềm.

Việc thiết lập mềm này cũng được thực hiện trên mỗi quá trình khởi động lại.

Nhóm công tác IGD định rõ rằng dịch vụ xác thực liên kết là dịch vụ con của dịch vụ cấu hình WLAN khi chứa trong thiết bị điểm truy cập WLAN. Do đó, khi hoạt động ResetAuthentication của dịch vụ cấu hình WLAN được gọi thì thực thi hoạt động ResetAuthentication của dịch vụ cấu hình WLAN phải gọi thực thi hoạt động ResetAuthentication của dịch vụ xác thực liên kết.

2.4.8.1 Các đối số

Không có thông tin.

2.4.8.2 Phụ thuộc vào trạng thái (nếu có)

2.4.8.3 Ảnh hưởng đến trạng thái (nếu có)

2.4.8.4 Các lỗi

Mã lỗi	Mô tả lỗi	Mô tả
402	Đối số không hợp lệ	Xem điều 2.4.22
501	Hoạt động thất bại	Xem điều 2.4.22

2.4.9 Các mã lỗi chung

Bảng sau đây liệt kê các mã lỗi chung cho các hoạt động về kiểu dịch vụ này. Nếu một hoạt động dẫn đến nhiều lỗi thì lỗi cụ thể nhất sẽ được trả về.

Bảng 10 - Các mã lỗi chung

Mã lỗi	Mô tả lỗi	Mô tả
401	Hoạt động không hợp lệ	Xem Kiến trúc thiết bị UPnP phần Điều khiển
402	Đối số không hợp lệ	Xem Kiến trúc thiết bị UPnP phần Điều khiển
404	Biến không hợp lệ	Xem Kiến trúc thiết bị UPnP phần điều khiển

Mã lỗi	Mô tả lỗi	Mô tả
501	Hoạt động thất bại	Xem Kiến trúc thiết bị UPnP phần điều khiển
600-699	Chưa xác định	Các lỗi hoạt động chung. Do Ban UPnP Forum Technical Committee xác định
701-799		Các lỗi hoạt động chung do các Ban UPnP Forum working committee xác định
800-899	*Chưa xác định*	*(do nhà cung cấp UPnP quy định)*

2.5 Lý thuyết vận hành

Dịch vụ xác thực liên kết cung cấp các cơ chế cho các điểm điều khiển nhằm mục đích truy cập bộ nhớ chứng thực theo từng máy trạm. Khuyến cáo rằng các hoạt động của dịch vụ này được điều khiển bằng cách sử dụng *DeviceSecurity:1.0* như đã xác định trong nhóm công tác an ninh UPnP. Thuật ngữ "per-client" có nghĩa là người sử dụng và hoặc các thiết bị máy trạm WLAN có chứng thực duy nhất, trái với việc sử dụng chứng thực chung toàn mạng đơn. Dịch vụ này có thể được sử dụng cho mọi cơ chế xác thực nhưng một trong các cách sử dụng chính là với chuẩn 802.1x. Các điều dưới đây mô tả cách hoạt động với chuẩn 802.1x ngoài ra cũng có thể áp dụng cho các quá trình xác thực khác, ví dụ mọi máy trạm có thể lưu trữ các khóa công khai trong bộ nhớ chứng thực được khóa lại với bộ định danh duy nhất của nó.

2.5.1 Giới thiệu chuẩn 802.x

IEEE 802.1x là khung tổng quát bắt buộc – giải đáp được sử dụng để truy cập ở mức gateway (như trong chuyển mạch Ethernet) tới mạng cục bộ. Có ba vai trò trong 802.1x 1) trình yêu cầu, 2) ký hiệu xác thực và 3) máy chủ xác thực. Trình yêu cầu là máy trạm cố gắng xác thực để truy cập mạng. Ký hiệu xác nhận là thiết bị bắt buộc xác thực và dịch vụ xác thực cung cấp cơ chế kiểm tra chứng thực của trình yêu cầu thay mặt cho ký hiệu xác nhận. Chuẩn 802.1x sử dụng EAP (Extensible Authentication Protocol – giao thức xác thực mở rộng) để trao đổi các thông điệp xác thực giữa máy trạm yêu cầu xác thực và máy chủ xác thực. Một vài giao thức xác thực EAP được quy định bao gồm EAP-TLS, Protected EAP, EAP-TTLS và các giao thức xác thực khác, xem RFC 2284 để biết thêm chi tiết. Với mỗi đặc tả 802.1x – "ký hiệu xác nhận và máy chủ xác thực có thể được định vị cùng nhau trong cùng một hệ thống, cho phép hệ thống đó thực hiện chức năng xác thực mà không yêu cầu giao tiếp với máy chủ bên ngoài" – IEEE Std 802.1x-2001 §6.1.

IEEE 802.1x được điều chỉnh cho phù hợp với 802.1x ở đó trạm không dây (trình yêu cầu) xác thực với máy chủ xác thực qua AP(ký hiệu xác nhận). Điều này được áp dụng trong các mạng doanh nghiệp ở đó các giao thức xác thực dựa vào các máy chủ xác thực "nền" (ví dụ: RADIUS).

Các máy chủ được liên kết với cơ sở dữ liệu người sử dụng được tìm thấy trong các mạng công ty do nhân viên IT quản trị. Tuy nhiên, không thể chắc chắn về trình độ của chuyên gia quản trị trong môi trường trong nhà. Dịch vụ xác thực liên kết cung cấp khung tổng quát cho máy chủ xác thực đơn giản và đầy đủ trong đó có thể được cập nhật qua các hoạt động UPnP. Mặc dù dịch vụ xác thực liên kết được giả thiết định vị cùng với AP nhưng nó có thể được chạy trên thiết bị riêng biệt trên LAN.

2.5.2 Hoạt động mức cao

Các điểm truy cập thực thi xác thực dựa trên chuẩn 802.1x yêu cầu sử dụng (các) máy chủ xác thực. Ngoài ra, các thiết bị máy trạm trong chuẩn 802.1x như là các thiết bị cài sẵn với chứng thực duy nhất được dựng sẵn hoặc cấu hình trước ("theo từng máy trạm") như là các mật khẩu hoặc các chứng thực yêu cầu có các chứng thực được xác minh, thêm và lưu trữ ban đầu trong máy chủ xác thực. Dịch vụ xác thực liên kết có thể được sử dụng bởi AP hỗ trợ chuẩn 802.1x và không có máy chủ xác thực như là biến RADIUS (bên ngoài thiết bị AP) trên mạng. Dịch vụ này cung cấp phương tiện các điểm điều khiển UPnP để lưu trữ và truy cập dữ liệu xác thực, khi đó thực chất là API trung gian để sửa đổi cơ sở dữ liệu xác thực thì AP sẽ sử dụng cho xác thực theo chuẩn 802.1x. Nó cũng cung cấp cơ chế thông báo đến điểm điều khiển qua các sự kiện UPnP mà một mục nhập riêng yêu cầu được xác nhận tính hợp lệ. Bộ lưu trữ dữ liệu xác thực có thể có mặt ở mọi nơi trên mạng. Ví dụ, nó có thể được lữu trữ trên AP hoặc trong thiết bị đã cài sẵn như là IGD trong đó có thể tạo dịch vụ xác thực liên kết hoặc cơ sở dữ liệu. Đối với trường hợp sau, AP có thể truy cập cơ sở dữ liệu trên IGD qua RADIUS và người sử dụng có thể thao tác cơ sở dữ liệu qua dịch vụ xác thực liên kết. RFC 2716 (EAP-TLS) sử dụng thuật ngữ "máy chủ EAP" để biểu thị "điểm cuối cùng" thực hiện quá trình xác thực. Thuật ngữ ngày cũng được sử dụng dưới đây.

Dịch vụ xác thực liên kết duy trì các bản ghi với các biến trạng thái nhằm trợ giúp các điểm điều khiển (qua tương tác người dùng cuối) trong việc xác minh, thêm và lưu trữ các chứng thực duy nhất cho mỗi người sử dụng hoặc mỗi thiết bị. Có hai thể hiện thay đổi các bản ghi trong cơ sở dữ liệu. Ví dụ, trong trường hợp dịch vụ xác thực liên kết và cơ sở dữ liệu thể hiện qua AP, một thể hiện là máy chủ 802.1x EAP trong khi thể hiện khác là điểm điều khiển UPnP. Cả hai có thể cập nhật các trường trong cơ sở dữ liệu xác thực và đáp ứng các thay đổi. Mọi sửa đổi cho các bản ghi của máy trạm tạo ra các sự kiện UPnP thích hợp (xem mô tả cho biến `LastChange`).

Dịch vụ này hỗ trợ các giao thức xác thực hữu hiệu nhất được quy định qua EAP của chuẩn 802.1x. Trong tiêu chuẩn này, các giao thức EAP được tạo thành hai kiểu. Kiểu đầu tiên yêu cầu khóa công khai của máy trạm được xác minh, kiểu thứ hai yêu cầu người sử dụng cuối nhập một secret như là mật khẩu. Ví dụ, với EAP-TLS certificate (chứng thực) của máy trạm được gửi đến cho AP và sau đó đến điểm điều khiển. Giả sử rằng người sử dụng tại điểm điều khiển có phương tiện để xác nhận tính hợp lệ của certificate này. Kiểu EAP khác là Protected EAP bao gồm đường hầm EAP-TLS với việc sử dụng giao thức bên trong như là MSCHAPv2. Trong

trường hợp này, secret/mật khẩu dùng chung được nhập qua điểm điều khiển và lưu trữ trong cơ sở dữ liệu. Secret có mặt trong máy trạm với bộ nhớ không giới hạn như là đĩa hoặc đặt trong bộ nhớ flash tại thời điểm điểm sản xuất. Ví dụ, secret trên thiết bị đóng/cài sẵn có thể được truy cập bởi người sử dụng bằng cách đọc nhãn trên thiết bị hoặc tài liệu đã in. Khi mà người sử dụng nhập secret vào điểm điều khiển thì nó sẽ được gửi đến AP và được sử dụng để xác thực máy trạm.

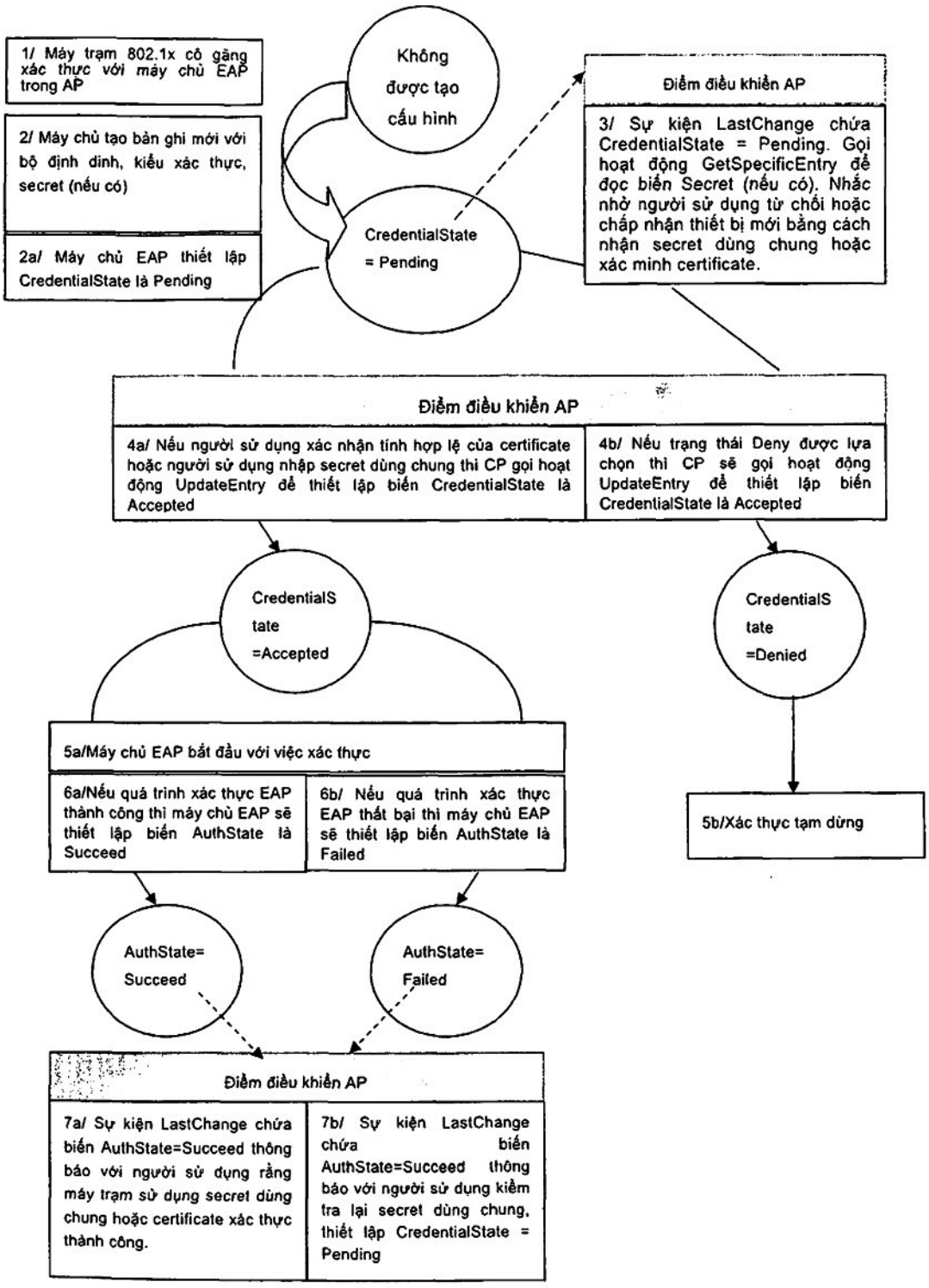
2.5.3 Hoạt động mức chi tiết

Quá trình của 802.1x EAP bắt đầu với một yêu cầu của máy chủ EAP cho chuỗi định danh EAP từ máy trạm đăng ký. Máy chủ EAP truy cập các bản ghi xác thực sử dụng chuỗi định danh EAP để nhận bản ghi với trường Identifier tương ứng. Do đó, tất cả các thiết bị truy cập mạng không dây phải có các chuỗi định danh EAP duy nhất. Sau đó, quá trình EAP tiến hành lựa chọn phương pháp xác thực (kiểu EAP). Khi mà kiểu EAP được máy chủ và máy trạm thông qua thì phương pháp xác thực EAP sẽ được thực hiện. Kỳ vọng rằng máy chủ EAP sẽ tham chiếu đến bản ghi của máy trạm tương ứng với trường Identifier cho trước trong suốt quá trình xác thực và xác minh rằng các chứng thực sử dụng cho việc xác thực sẽ phù hợp trong các bản ghi xác thực đó.

Nếu chuỗi định danh EAP không phù hợp với mọi trường `Identifiers` của máy trạm thì bản ghi mới sẽ được tạo bởi máy chủ EAP. Máy chủ EAP nên điền vào bản ghi với trường `Identifier` thiết lập chuỗi định danh EAP từ máy trạm đăng ký và thiết lập `AuthType` tương ứng với chế độ xác thực EAP (như là EAP-TLS) được lựa chọn bởi máy chủ EAP. Máy chủ EAP cũng cập nhật trường địa chỉ MAC trong bản ghi. Nếu các trao đổi chứng thực xảy ra trong trường hợp EAP-TLS vào thời điểm này thì máy chủ EAP sẽ điền trường `Secret`. Máy chủ EAP có thể thiết lập trường `CredentialState` là `Pending` trong đó kích khởi trường `LastChange` và thông báo các điểm điều khiển của máy trạm đăng ký. Các điểm điều khiển sẽ nhắc người sử dụng chấp nhận hoặc từ chối các chứng thực máy trạm. Nếu người sử dụng lựa chọn `Denied` thì điểm điều khiển sẽ gọi hoạt động `UpdateEntry`, tạm ngưng quá trình xác thực máy trạm. Điều này dẫn đến việc EAP sẽ không được gửi đến máy trạm bởi AP. Nếu người sử dụng lựa chọn `Accepted` thì việc xác thực máy trạm tiếp tục và máy chủ EAP xác minh chứng thực trong trường secret đang được sử dụng cho việc xác thực máy trạm. Tại thời điểm kết thúc quá trình xác thực máy chủ EAP cập nhật trường `AuthState`.

Tuy nhiên, nếu định danh EAP phù hợp với trường `Identifier` và `CredentialState` thì máy chủ EAP sẽ bắt đầu với quá trình xác thực và xác minh chứng thực trong trường secret đang được sử dụng cho việc xác thực máy trạm. Nếu trường `CredentialState` là `Denied` thì quá trình xác thực máy trạm tạm ngưng và EAP sẽ không được gửi đến máy trạm. Tại thời điểm kết thúc quá trình xác thực máy chủ EAP cập nhật trường `AuthState`.

Máy chủ EAP/Xác thực liên kết/ tương tác điểm điều khiển AP với thiết bị mới đang cố gắng xác thực



Các mũi tên nét đứt cho biết cách thay đổi trong các biến CredentialState và AuthState được xử lý tại điểm điều khiển. Các mũi tên nét liền cho biết các thay đổi hợp lệ cho các biến CredentialState và AuthState bởi điểm điều khiển và máy chủ EAP.

2.5.4 Định dạng bản ghi

Mỗi bản ghi được ghi địa chỉ duy nhất qua trường `Identificr`. Giống như một ví dụ, các bản ghi xác thực sau đây chứa hai bản ghi thiết bị với `CredentialState` đặt là `Accepted`, có tên là thiết bị 1 và thiết bị 2. Đối với ví dụ này, hai thiết bị này xác thực qua EAP-TLS và AP lưu trữ các khóa công khai của thiết bị. Biến `AuthState` có giá trị `Authenticated` khi một trong hai thiết bị này gửi định danh EAP của nó, AP sẽ tìm bản ghi phù hợp và so sánh các nội dung của trường Secret với khóa công khai mà máy trạm gửi trong suốt giai đoạn TLS handshake.

Trường Indentifier	**Trường Secret**	**Kiểu Secret**	**Kiểu xác thực**	**Trạng thái chứng thực**	**Trạng thái xác thực**	**Mô tả**	**Địa chỉ MAC**	**Thời gian chứng thực**
Thiết bị 1	Khóa 1	Khóa công khai	Xác nhận tính hợp lệ của chứng thực	Accepted	Succeeded		MAC 1	0
Thiết bị 2	Khóa 2	Khóa công khai	Xác nhận tính hợp lệ của chứng thực	Accepted	Succeeded		MAC 1	0
...	...	...	...		...	...	...	...

Với EAP-TLS trường Identifier và khóa công khai sẽ được gửi qua liên kết không dây trong suốt giai đoạn TLS handshake. TLS sẽ đảm bảo rằng máy trạm gửi khóa công khai có khóa bí mật phù hợp. Điều quan trọng là lưu trữ và so sánh chứng thực đối với EAP-TLS, ở ví dụ về khóa công khai này, trong các bản ghi xác thực với khóa công khai của máy trạm khi một thiết bị bí ẩn có thể giả mạo thiết bị 1 bằng cách gửi thiết bị 1 như bộ định danh của nó và sử dụng địa chỉ MAC của thiết bị 1. Ngoài ra, thiết bị bí ẩn có thể dễ dàng tạo một cặp khóa công khai/ khóa bí mật hợp lệ cho AP trong suốt giai đoạn TLS handshake. Nếu khóa công khai của máy trạm bí ẩn không phù hợp với trường Secret xác thực người sử dụng của thiết bị 1 (khóa công khai của nó) trong các bản ghi xác thực thì máy chủ AP EAP sẽ đòi hỏi thiết bị bí ẩn sử dụng khóa công khai của nó và máy trạm sẽ thành giai đoạn TLS handshake. Do đó, để ngăn ngừa các thiết bị bí ẩn khỏi việc giả

mạo bằng cách sử dụng các khóa của chúng, khóa công khai hoặc chứng thực khác nên được duy trì trong các bản ghi xác thực và phù hợp trong suốt quá trình xác thực.

2.5.5 Ví dụ sử dụng các chứng thực chứng chỉ máy trạm

Trong ví dụ này, thiết bị máy trạm dựa vào chuẩn 802.1x đang cố gắng truy cập mạng. Giả sử máy trạm và AP đều được tạo cấu hình với các chứng thực từ thẩm quyền chứng thực chung. Quá trình EAP-TLS sẽ trao đổi các thử thách và các chứng thực. Các chứng thực được xác nhận tính hợp lệ về ngày hết hạn và chuỗi chứng thực của thẩm quyền chứng nhận gốc. Trong trường hợp này, chứng thực AP được xác nhận tính hợp lệ bởi máy trạm sau đó tiếp tục với việc thiết lập đường hầm TLS. Thời điểm ban đầu máy trạm kết hợp AP được giả định tìm ra chứng thực máy trạm (hoặc hàm băm của khóa công khai trong chứng thực) không có trong các bản ghi chứng thực máy trạm. Trong trường hợp này, máy chủ EAP tạo và phổ biến một bản ghi với các trường `Identifier`, `secret` và `AuthType of ValidateCredentials`, sau đó máy chủ EAP thiết lập biến `CredentialState` là `Pending`. CP nhận (các) sự kiện và thông báo với người sử dụng rằng thiết bị với bộ định danh của (chuỗi ví dụ như số seri của nhà sản xuất) và "secret" của (một số chuỗi) yêu cầu truy cập mạng. Biến secret trong trường hợp này được in ở đáy của thiết bị máy trạm. Đây là hàm băm của khóa công khai. Người sử dụng sẽ quan sát bên dưới thiết bị và kiểm tra sự phù hợp giữa số trên nhãn với số trên điểm điều khiển. Nếu các số phù hợp với nhau thì người sử dụng sẽ kích vào nút "accepted" và nhập một khoảng thời gian truy cập tạm thời. CP sẽ thiết lập `CredentialState` là `Accepted` và máy chủ EAP sẽ tiếp tục phiên TLS đảm bảo khóa công khai từ máy trạm được sử dụng cho phiên TLS. Dù xác thực EAP-TLS thành công hay thất bại thì biến `AuthState` sẽ được cập nhật thông báo cho điểm điều khiển. Chú ý máy trạm được xác thực bởi AP (bằng cách kiểm tra hàm băm trên thiết bị).

Ví dụ trên dựa vào các máy trạm và AP có các chứng thực cài trước. điều này không thiết thực với mạng trong nhà nhất là đối với các thiết bị nhỏ không có giao diện người sử dụng. Thông tin này sẽ phải được ghi địa chỉ với một số phương pháp xác thực nhằm cung cấp xác thực chung nhưng không yêu cầu xác nhận tính hợp lệ của chứng thực.

2.5.6 Các giới hạn trên bản ghi treo

Máy chủ EAP phải xóa các bản ghi `Pending` khi quá trình xác thực dựa vào chuẩn 802.1x bị hủy bỏ. Các máy trạng thái và các giá trị thời gian được quy định trong IEEE Std 802.1x-2001.

Kẻ tấn công có thể xác thực với việc lựa chọn ngẫu nhiên các chuỗi định danh EAP và áp đảo bộ lưu trữ chứng thực bằng cách tạo rất nhiều bản ghi `Pending`. Mỗi thực thi nên đặt một giới hạn phụ thuộc trên số lượng tối đa các bản ghi `pending`.

3 Mô tả dịch vụ bằng XML

```
<?xml version="1.0"?>
<scpd xmlns="urn:schemas-upnp-org:service-1-0">
      <specVersion>
            <major>1</major>
```

```
      <minor>0</minor>
</specVersion>
<actionList>
      <action>
            <name>GetGenericEntry</name>
            <argumentList>
                  <argument>
                        <name>NewIndex</name>
                        <direction>in</direction>
                        <relatedStateVariable>NumberOfEntries</relatedStateVa
                        riable>
                   </argument>
                   <argument>
                        <name>NewIdentifier</name>
                        <direction>out</direction>
                        <relatedStateVariable>Identifier</relatedStateVariabl
                   e>
                   </argument>
                   <argument>
                        <name>NewSecret</name>
                        <direction>out</direction>
                        <relatedStateVariable>Secret</relatedStateVariable>
                   </argument>
                   <argument>
                        <name>NewSecretType</name>
                        <direction>out</direction>
                        <relatedStateVariable>SecretType</relatedStateVariabl
                   e>
                   </argument>
                   <argument>
                        <name>NewAuthType</name>
                        <direction>out</direction>
                        <relatedStateVariable>AuthType</relatedStateVariable>
                   </argument>
                   <argument>
                       <name>NewAuthState</name>
                       <direction>out</direction>
                       <relatedStateVariable>AuthState</relatedStateVariable>
                   </argument>
                   <argument>
                        <name>NewCredentialState</name>
                        <direction>out</direction>

                        <relatedStateVariable>CredentialState</relatedStateVa
                        riable>
                   </argument>
                  <argument>
                        <name>NewDescription</name>
                        <direction>out</direction>
                         <relatedStateVariable>Description</relatedStateVariab
                         le>
                  </argument>
                  <argument>
                      <name>NewMACAddress</name>
                      <direction>out</direction>
                      <relatedStateVariable>MACAddress</relatedStateVariable>
                   </argument>
                   <argument>
                      <name>NewCredentialDuration</name>
```

```
                    <direction>out</direction>
                    <relatedStateVariable>CredentialDuration</relatedStateVaria
                    ble>
                   </argument>
              <argument>
                   <name>NewLinkedIdentifier</name>
                   <direction>out</direction>
                    <relatedStateVariable>LinkedIdentifier</relatedStateVariabl
                    e>
             </argument>
        </argumentList>
    </action>
    <action>
        <name>GetSpecificEntry</name>
        <argumentList>
            <argument>
                   <name>NewIdentifierKey</name>
                   <direction>in</direction>
                   <relatedStateVariable>Identifier</relatedStateVariable>
            </argument>
            <argument>
                   <name>NewIdentifier</name>
                   <direction>out</direction>
                   <relatedStateVariable>Identifier</relatedStateVariable>
            </argument>
            <argument>
                   <name>NewSecret</name>
                   <direction>out</direction>
                   <relatedStateVariable>Secret</relatedStateVariable>
            </argument>
            <argument>
                   <name>NewSecretType</name>
                   <direction>out</direction>
                   <relatedStateVariable>SecretType</relatedStateVariable>
            </argument>
            <argument>
                   <name>NewAuthType</name>
                   <direction>out</direction>
                   <relatedStateVariable>AuthType</relatedStateVariable>
            </argument>
            <argument>
                   <name>NewAuthState</name>
                   <direction>out</direction>
                   <relatedStateVariable>AuthState</relatedStateVariable>
            </argument>
            <argument>
                    <name>NewCredentialState</name>
                    <direction>out</direction>
                    <relatedStateVariable>CredentialState</relatedStateVariable>
            </argument>
            <argument>
                    <name>NewDescription</name>
                    <direction>out</direction>
                    <relatedStateVariable>Description</relatedStateVariable>
            </argument>
            <argument>
                    <name>NewMACAddress</name>
                    <direction>out</direction>
                    <relatedStateVariable>MACAddress</relatedStateVariable>
            </argument>
            <argument>
                    <name>NewCredentialDuration</name>
                    <direction>out</direction>
```

```
                <relatedStateVariable>CredentialDuration</relatedStateVaria
                ble>
        </argument>
        <argument>
                <name>NewLinkedIdentifier</name>
                <direction>out</direction>
                <relatedStateVariable>LinkedIdentifier</relatedStateVariable>
        </argument>
    </argumentList>
</action>
<action>
    <name>AddEntry</name>
    <argumentList>
        <argument>
            <name>NewIdentifier</name>
            <direction>in</direction>
            <relatedStateVariable>Identifier</relatedStateVariable>
        </argument>
        <argument>
            <name>NewSecret</name>
            <direction>in</direction>
            <relatedStateVariable>Secret</relatedStateVariable>
        </argument>
        <argument>
            <name>NewSecretType</name>
            <direction>in</direction>
            <relatedStateVariable>SecretType</relatedStateVariable>
        </argument>
        <argument>
            <name>NewAuthType</name>
            <direction>in</direction>
            <relatedStateVariable>AuthType</relatedStateVariable>
        </argument>
        <argument>
            <name>NewAuthState</name>
            <direction>in</direction>
            <relatedStateVariable>AuthState</relatedStateVariable>
        </argument>
        <argument>
            <name>NewCredentialState</name>
            <direction>in</direction>
            <relatedStateVariable>CredentialState</relatedStateVariable>
        </argument>
        <argument>
            <name>NewDescription</name>
            <direction>in</direction>
            <relatedStateVariable>Description</relatedStateVariable>
        </argument>
        <argument>
            <name>NewMACAddress</name>
            <direction>in</direction>
            <relatedStateVariable>MACAddress</relatedStateVariable>
        </argument>
        <argument>
            <name>NewCredentialDuration</name>
            <direction>in</direction>
             <relatedStateVariable>CredentialDuration</relatedStateVaria
             ble>
        </argument>
        <argument>
             <name>NewLinkedIdentifier</name>
             <direction>in</direction>
             <relatedStateVariable>LinkedIdentifier</relatedStateVariabl
             e>
```

```
            </argument>
            <argument>
                <name>NewNumberOfEntries</name>
                <direction>out</direction>
                <relatedStateVariable>NumberOfEntries</relatedStateVariable>
            </argument>
        </argumentList>
    </action>
    <action>
        <name>UpdateEntry</name>
        <argumentList>
            <argument>
                <name>NewIdentifier</name>
                <direction>in</direction>
                <relatedStateVariable>Identifier</relatedStateVariable>
            </argument>
            <argument>
                <name>NewSecret</name>
                <direction>in</direction>
                <relatedStateVariable>Secret</relatedStateVariable>
            </argument>
            <argument>
                <name>NewSecretType</name>
                <direction>in</direction>
                <relatedStateVariable>SecretType</relatedStateVariable>
            </argument>
            <argument>
                <name>NewAuthType</name>
                <direction>in</direction>
                <relatedStateVariable>AuthType</relatedStateVariable>
            </argument>
            <argument>
                <name>NewAuthState</name>
                <direction>in</direction>
                <relatedStateVariable>AuthState</relatedStateVariable>
            </argument>
            <argument>
                <name>NewCredentialState</name>
                <direction>in</direction>
                <relatedStateVariable>CredentialState</relatedStateVariable>
            </argument>
            <argument>
                <name>NewDescription</name>
                <direction>in</direction>
                <relatedStateVariable>Description</relatedStateVariable>
            </argument>
            <argument>
                <name>NewMACAddress</name>
                <direction>in</direction>
                <relatedStateVariable>MACAddress</relatedStateVariable>
            </argument>
            <argument>
                <name>NewCredentialDuration</name>
                <direction>in</direction>
                <relatedStateVariable>CredentialDuration</relatedStateVariable>
            </argument>
            <argument>
                <name>NewLinkedIdentifier</name>
                <direction>in</direction>
                <relatedStateVariable>LinkedIdentifier</relatedStateVariable>
            </argument>
            <argument>
                <name>NewNumberOfEntries</name>
                <direction>out</direction>
```

```
                <relatedStateVariable>NumberOfEntries</relatedStateVariable>
            </argument>
        </argumentList>
    </action>
    <action>
        <name>DeleteEntry</name>
        <argumentList>
            <argument>
                <name>NewIdentifier</name>
                <direction>in</direction>
                <relatedStateVariable>Identifier</relatedStateVariable>
            </argument>
            <argument>
                <name>NewNumberOfEntries</name>
                <direction>out</direction>
                <relatedStateVariable>NumberOfEntries</relatedStateVariable>
            </argument>
        </argumentList>
    </action>
    <action>
        <name>GetNumberOfEntries</name>
        <argumentList>
            <argument>
                <name>NewNumberOfEntries</name>
                <direction>out</direction>
                <relatedStateVariable>NumberOfEntries</relatedStateVariable>
            </argument>
        </argumentList>
    </action>
    <action>
        <name>FactoryDefaultReset</name>
    </action>
    <action>
        <name>ResetAuthentication</name>
    </action>
</actionList>
<serviceStateTable>
<stateVariable sendEvents="no">
    <name>NumberOfEntries</name>
    <dataType>ui2</dataType>
    <defaultValue>0</defaultValue>
</stateVariable>
<stateVariable sendEvents="no">
    <name>Identifier</name>
    <dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="no">
    <name>Secret</name>
    <dataType>string</dataType>
</stateVariable>
<stateVariable sendEvents="no">
    <name>SecretType</name>
    <dataType>string</dataType>
    <allowedValueList>
        <allowedValue>TextPassword</allowedValue>
        <allowedValue>X509Certificate</allowedValue>
        <allowedValue>PublicKey</allowedValue>
        <allowedValue>PublicKeyHash160</allowedValue>
    </allowedValueList>
</stateVariable>
<stateVariable sendEvents="no">
    <name>AuthType</name>
    <dataType>string</dataType>
    <allowedValueList>
```

```
            <allowedValue>SharedSecret</allowedValue>
            <allowedValue>ValidateCredentials</allowedValue>
        </allowedValueList>
    </stateVariable>
    <stateVariable sendEvents="no">
        <name>AuthState</name>
        <dataType>string</dataType>
        <defaultValue>Unconfigured</defaultValue>
        <allowedValueList>
            <allowedValue>Unconfigured</allowedValue>
            <allowedValue>Failed</allowedValue>
            <allowedValue>Succeeded</allowedValue>
        </allowedValueList>
    </stateVariable>
    <stateVariable sendEvents="no">
        <name>CredentialState</name>
        <dataType>string</dataType>
        <defaultValue>Unconfigured</defaultValue>
        <allowedValueList>
            <allowedValue>Unconfigured</allowedValue>
            <allowedValue>Pending</allowedValue>
            <allowedValue>Accepted</allowedValue>
            <allowedValue>Denied</allowedValue>
        </allowedValueList>
    </stateVariable>
    <stateVariable sendEvents="no">
        <name>Description</name>
        <dataType>string</dataType>
    </stateVariable>
    <stateVariable sendEvents="no">
        <name>MACAddress</name>
        <dataType>string</dataType>
    </stateVariable>
    <stateVariable sendEvents="no">
        <name>CredentialDuration</name>
        <dataType>ui4</dataType>
        <defaultValue>0</defaultValue>
    </stateVariable>
    <stateVariable sendEvents="yes">
        <name>LastChange</name>
        <dataType>string</dataType>
    </stateVariable>
    <stateVariable sendEvents="no">
        <name>LinkedIdentifier</name>
        <dataType>string</dataType>
    </stateVariable>
    <stateVariable sendEvents="yes">
        <name>LastError</name>
        <dataType>string</dataType>
    </stateVariable>
</serviceStateTable>
```

</scpd

4 Kiểm thử

Không có các kiểm thử về ngữ nghĩa nào được xác định trong dịch vụ này.

Phụ lục A

(Tham khảo)

Các tiêu chuẩn gốc về UPnP

Trong tiêu chuẩn này, có thể tạo ra tham chiếu đến các tiêu chuẩn gốc UPnP. Các tham chiếu này nhằm mục đích duy trì tính nhất quán giữa các đặc tả do ISO/IEC và hiệp hội các nhà thực thi UPnP công bố. Bảng sau đây chỉ ra các tiêu đề tiêu chuẩn UPnP và phần tương ứng của TCVN 10176 (ISO/IEC 29341)

Tiêu đề tiêu chuẩn về UPnP	Tiêu chuẩn tương ứng
Kiến trúc thiết bị UPnP phiên bản 1.0	(ISO/IEC 29341-1)
Thiết bị cơ sở UPnP	(ISO/IEC 29341-2)
Kiến trúc âm thanh và hình ảnh	(ISO/IEC 29341-3-1)
Thiết bị kết xuất media	(ISO/IEC 29341-3-2)
Thiết bị máy chủ media	(ISO/IEC 29341-3-3)
Dịch vụ vận tải âm thanh và hình ảnh	(ISO/IEC 29341-3-10)
Dịch vụ quản lý kết nối	(ISO/IEC 29341-3-11)
Dịch vụ thư mục nội dung	(ISO/IEC 29341-3-12)
Dịch vụ kiểm soát kết xuất	(ISO/IEC 29341-3-13)
Thiết bị kết xuất media mức 2	(ISO/IEC 29341-4-2)
Dịch vụ máy chủ media mức 2	(ISO/IEC 29341-4-3)
Khuôn mẫu cấu trúc dữ liệu	(ISO/IEC 29341-4-4)
Dịch vụ vấn tải âm thanh và hình ảnh mức 2	(ISO/IEC 29341-4-10)
Dịch vụ quản lý kết nối mức 2	(ISO/IEC 29341-4-11)
Dịch vụ thư mục nội dung mức 2	(ISO/IEC 29341-4-12)
Dịch vụ kiểm soát kết xuất mức 2	(ISO/IEC 29341-4-13)
Ghi chép định kỳ mức 2	(ISO/IEC 29341-4-14)
Thiết bị camera an ninh số	(ISO/IEC 29341-5-1)
Dịch vụ chụp ảnh động an ninh số	(ISO/IEC 29341-5-10)
Dịch vụ cài đặt camera an ninh số	(ISO/IEC 29341-5-11)
Thiết bị hệ thống	TCVN 10176-6-1 (ISO/IEC 29341-6-1)

Thiết bị điều nhiệt theo vùng	TCVN 10176-6-2 (ISO/IEC 29341-6-2)
Dịch vụ van điều khiển	TCVN 10176-6-10 (ISO/IEC 29341-6-10)
Dịch vụ chế độ vận hành quạt	TCVN 10176-6-11 (ISO/IEC 29341-6-11)
Dịch vụ tốc độ quạt	TCVN 10176-6-12 (ISO/IEC 29341-6-12)
Dịch vụ trạng thái tòa nhà	TCVN 10176-6-13 (ISO/IEC 29341-6-13)
Dịch vụ lịch biểu điểm đặt	TCVN 10176-6-14 (ISO/IEC 29341-6-14)
Dịch vụ cảm biến nhiệt độ	TCVN 10176-6-15 (ISO/IEC 29341-6-15)
Dịch vụ điểm đặt nhiệt độ	TCVN 10176-6-16 (ISO/IEC 29341-6-16)
Dịch vụ chế độ người sử dụng	TCVN 10176-6-17 (ISO/IEC 29341-6-17)
Thiết bị chiếu sáng nhị phân	TCVN 10176-7-1 (ISO/IEC 29341-7-1)
Thiết bị chiếu sáng có thể điều chỉnh	TCVN 10176-7-2 (ISO/IEC 29341-7-2)
Dịch vụ điều chỉnh	TCVN 10176-7-10 (ISO/IEC 29341-7-10)
Dịch vụ chuyển mạch nguồn	TCVN 10176-7-11 (ISO/IEC 29341-7-11)
Thiết bị internet gateway	TCVN 10176-8-1 (ISO/IEC 29341-8-1)
Thiết bị mạng cục bộ	TCVN 10176-8-2 (ISO/IEC 29341-8-2)
Thiết bị mạng diện rộng	TCVN 10176-8-3 (ISO/IEC 29341-8-3)
Thiết bị kết nối mạng diện rộng	TCVN 10176-8-4 (ISO/IEC 29341-8-4)
Thiết bị điểm truy cập mạng cục bộ không dây	TCVN 10176-8-5 (ISO/IEC 29341-8-5)
Dịch vụ quản lý cấu hình host mạng cục bộ	TCVN 10176-8-10 (ISO/IEC 29341-8-10)
Dịch vụ chuyển tiếp tầng 3	TCVN 10176-8-11 (ISO/IEC 29341-8-11)
Dịch vụ xác thực liên kết	TCVN 10176-8-12 (ISO/IEC 29341-8-12)
Dịch vụ radius từ máy trạm	TCVN 10176-8-13 (ISO/IEC 29341-8-13)
Dịch vụ cấu hình liên kết cáp WAN	(ISO/IEC 29341-8-14)
Dịch vụ cấu hình giao diện chung cho WAN	(ISO/IEC 29341-8-15)
Dịch vụ cấu hình liên kết DSL(Kênh thuê bao số) WAN	(ISO/IEC 29341-8-16)
Dịch vụ cấu hình liên kết Ethernet WAN	(ISO/IEC 29341-8-17)
Dịch vụ kết nối IP WAN	(ISO/IEC 29341-8-18)

Dịch vụ cấu hình liên kết OTS WAN	(ISO/IEC 29341-8-19)
Dịch vụ kết nối PPP WAN	(ISO/IEC 29341-8-20)
Dịch vụ cấu hình WLAN	(ISO/IEC 29341-8-21)
Thiết bị máy in	(ISO/IEC 29341-9-1)
Thiết bị máy quét hình phiên bản 1.0	(ISO/IEC 29341-9-2)
Dịch vụ hoạt động ngoài	(ISO/IEC 29341-9-10)
Dịch vụ nạp	(ISO/IEC 29341-9-11)
Dịch vụ in cơ bản	(ISO/IEC 29341-9-12)
Dịch vụ quét hình	(ISO/IEC 29341-9-13)
Kiến trúc QoS phiên bản 1.0	(ISO/IEC 29341-10-1)
Dịch vụ thiết bị QoS	(ISO/IEC 29341-10-10)
Dịch vụ quản lý QoS	(ISO/IEC 29341-10-11)
Dịch vụ lưu trữ chính sách QoS	(ISO/IEC 29341-10-12)
Kiến trúc QoS mức 2	(ISO/IEC 29341-11-1)
Các lược đồ QoS	(ISO/IEC 29341-11-2)
Dịch vụ thiết bị QoS mức 2	(ISO/IEC 29341-11-10)
Dịch vụ quản lý QoS	(ISO/IEC 29341-11-11)
Dịch vụ lưu trữ chính sách QoS mức 2	(ISO/IEC 29341-11-12)
Thiết bị Client giao diện người sử dụng từ xa	(ISO/IEC 29341-12-1)
Thiết bị server giao diện người sử dụng từ xa	(ISO/IEC 29341-12-2)
Dịch vụ Client giao diện người sử dụng từ xa	(ISO/IEC 29341-12-10)
Dịch vụ server giao diện người sử dụng từ xa	(ISO/IEC 29341-12-11)
Dịch vụ an ninh cho thiết bị	(ISO/IEC 29341-13-10)
Dịch vụ điều khiển an ninh	(ISO/IEC 29341-13-11)