**WLANAccessPointDevice:1**

**1. Prehľad a rozsah**

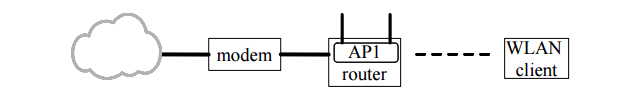
Šablóna tohto zariadenia vyhovuje UPnP architektúre, verzii 1.0.

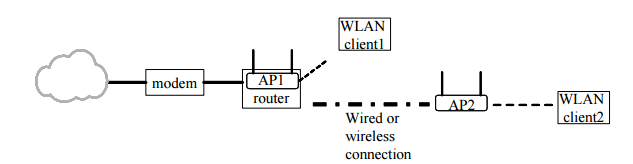
Tento dokument definuje požadované koreňové zariadenie   
*urn:schemas-upnp-org:device:WLANAccessPointDevice*.

*WLANAccessPointDevice* zapuzdruje služby pre Access Point Device Control Protocol (DCP).

Bezdrôtový LAN (WLAN) prístupový bod (Access Point, AP) je zariadenie, ktoré implementuje IEEE 802.11 (a, b, g) bezdrôtové štandardy, aby zabezpečil infraštruktúru siete pre domácnosť alebo malú firmu. Definícia zariadenia nezahŕňa používanie AP v hotspotoch alebo v podnikových sieťach.

AP sa správa ako Ethernertový most (bridge), ktorý povoľuje pripojenie viacerých uzlov do LAN. Obrázok 1a znázorňuje bežnú topológiu, použitú pre sieť s WLAN AP. Obrázok 1b zobrazuje použitie AP, ktorý predlžuje dosah siete LAN. DCP pokrýva oba tieto prípady.



**Obrázok 1a: WLANAccessPointDevice – bežný model použitia**

**Obrázok 1b: Predĺženie existujúcej siete – príklad topológie**

**1.1. Zameranie a ciele pre DCP verziu 1.0**

Pracovná skupina pre IGD (The Internet Gateway Device) sa rozhodla zamerať na nasledujúcu množinu funkcionalít spolu so službami pre AP DCP v 1.0.

* Konfigurovanie a dopytovanie 802.11 AP parametrov.
* Samozavádzanie bezpečnosti odkazu pre WLAN-y, ktoré používajú AP, založený na 802.11. Toto zahŕňa bezpečnosť predstavenia bezdrôtového klienta a AP zariadenia. Cieľom je vytvoriť jednoduché nastavenie a konfiguráciu WLAN bezpečnosti pre 802.11 AP a spravovanie WLAN prístupovej autorizácie.

**1.2. Čo DCP vo verzii 1.0 nezahŕňa**

Nasledujúce prediskutované body nespadajú do tejto verzie DCP:

* Nahradenie alebo posilnenie mechanizmu bezpečnosti odkazu poskytovaného AP
* Konfigurácia služieb pre AP v hotspotoch alebo v podnikových sieťach

**1.3. WLAN bezpečnostné požiadavky a odporúčania**

Bezpečnosť odkazu je kritická pre bezdrôtové domáce siete, pretože pripojenosť nie je obmedzená dosahom káblov alebo dostupnosťou fyzických portov. Pravdepodobnosť neúmyselných cross-  
-linkových a zákerných drive-by útokov bude stúpať s popularitou sietí WLAN. Toto narúša pohodlie užívateľa pri používaní bezdrôtovej siete a prekáža predstaveniu nových produktových kategórií a modelov využitia. Používatelia a poskytovatelia požadujú bezpečnosť odkazu ako súčasť balíka siete WLAN.

Alternatívou k bezpečnosti odkazu je chránenie špecifických zdrojov pomocou bezpečnostných mechanizmov, ktoré zahŕňajú vyššie (sieťovú alebo aplikačnú) vrstvy sieťového modelu. Od bežného domáceho užívateľa nemôžeme očakávať, že je technicky zručný a schopný identifikovať všetky zraniteľné body (dáta/zariadenia) v domácej sieti a ochrániť ich individuálne s primeranými metódami.

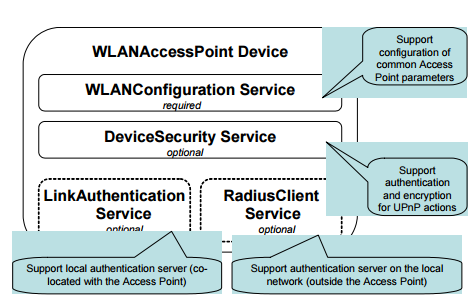
Momentálne najbežnejší spôsob, ako zabezpečiť 802.11 odkazy doma, zahŕňa Wired-Equivalent Privacy (WEP), založené na šifrovaní a autentizácii. Bezpečnostné riziká spojené s WEP sú všeobecne známe. Útočník môže rozlúštiť WEP kľúč zachycovaním balíkov pomocou bezdrôtového „očuchávania balíkov“ a pomocou široko dostupných možností určiť WEP kľúč. Ak vlastník WLAN nadobudne podozrenie kompromitovania bezpečnosti, WEP kľúč na všetkých užívateľských zariadeniach a AP musí byť obnovovaný, keďže rovnaký kľúč je používaný pre všetky uzly.

V rámci budovania zákazníckej dôvery a rozšírenia použitia bezdrôtových aplikácií je dôležité, aby si domáce WLAN zariadenia osvojili bezpečnejšie mechanizmy, napríklad Wireless Protected Access (WPA), ktorý je momentálne navrhovaný do oblasti 802.11. Z dlhodobého hľadiska sa očakáva, že bezpečnostné špecifikácie, spracované do kategórie 802.11i, budú široko prijaté a budú primeraným riešením pre silné bezpečnostné mechanizmy v AP. Vylepšená bezpečnosť poskytuje autentizáciu každého užívateľa, kľúče pre každú reláciu (session), pravidelné menenie kľúčov a bezpečnejšie šifrovacie metódy, ako Advanced Encryption Standard (AES).

Jeden z hlavných problémov s používaním bezpečnosti v sieťach WLAN je proces nastavovania bezpečnostných parametrov. Súčasné mechanizmy, používané pre inicializovanie bezpečnosti odkazu v AP zariadení nie sú veľmi user-friendly. Napríklad, s modelom WEP, užívateľ musí získať dlhý WEP kľúč pre AP, takže ho najprv získa cez bezpečné/drôtové pripojenie, a potom ho korektne vloží novému klientovi. Tento problém svojpomocného riešenia taktiež existuje aj s mechanizmami, navrhnutými ako vylepšenie základnej bezpečnosti založenej na WEP. Vďaka tomu užívateľ zvyčajne nenastaví bezpečnosť v sieti, čo vedie k zraniteľnosti siete. Cieľom bezpečnostnej inicializácie je mechanizmus, používajúci UPnP™ technológiu, navrhnutý v tomto dokumente, ktorý minimalizuje zapojenie užívateľa a predstavuje intuitívny model použitia pre užívateľov tak, aby získali úroveň bezpečnosti, ktorú AP dokáže poskytnúť.

Celkové bezpečnostné riešenie by malo chrániť užívateľa pred „man-in-the-middle“ útokmi tým, že predchádza spojeniu užívateľovho klienta s nepriateľským AP a užívateľov AP od spojenia s cudzím klientom. Malo by predchádzať „session-hijack“ útokom overovaním, či všetky správy medzi AP a klientom sú autentizované. Nemalo by byť náchylné k „dictionary“ útokom, napríklad útočník rozlúšti heslo po „sniffing“ (čuchacej) výmene výzvy a odpovede z protokolu, založeného na hesle.

Cieľom DCP je umožniť bezpečné WLAN riešenie s AP zariadením, ktoré implementuje požadované elementy špecifikované v DCP. Nasledujúci obrázok zobrazuje základné funkčné komponenty *WLANAccessPointDevice* zariadenia.



**Obrázok 2: Funkčné komponenty *WLANAccessPointDevice* zariadenia**

**1.3.1 AP konfigurácia parametrov**

*WLANConfiguration* služba, ktorá je povinná pre zariadenie *WLANAccessPointDevice*, poskytuje stavové premenné pre niektoré AP parametre, ktoré tím vývojárov považoval za užitočné pre konfiguráciu cez UPnP™ klienta. Poskytujú možnosť jednoduchej konfigurácie bezpečnosti a operačných parametrov, ponúka diagnostické informácie a pomáha nastaviť funkciu prevádzača. Naviac, technológia UPnP™ poskytuje aj možnosť notifikácií o udalostiach na informovanie klientov, ktorí majú záujem o stav AP. S AP, ktorý neposkytuje UPnP™ technológiu, užívatelia môžu mať prístup k niektorým parametrom cez webový prehliadač bez bezpečnostných mechanizmov autentizácie a kontrol prístupu. Taktiež proces konfigurácie medzi AP a klientom nie je chránený diskrétnosťou a sú zraniteľné voči útokom.

Veľmi sa odporúča pre AP, aby mal DCP mechanizmy na autentizáciu prístupu pre procesy UPnP™, a taktiež poskytoval diskrétnosť dát. Tiež sa odporúča mať mechanizmus, ktorý vynechá neautentizované a neoverené prístupy k parametrom, ktoré môžu byť prístupné len bezpečným UPnP™ procesom. Bez takejto kontroly prístupu každé klientske zariadenie v sieti LAN môže zmeniť nastavenia AP, čím ovplyvní celú sieť. Toto sa zvlášť týka prostredia malých podnikov. Obmedzenie povolenia zápisu v AP parametroch zníži bremeno podpory dodávateľa vybavenia siete a poskytovateľa služieb.  
Odporúča sa použiť opatrenia, definované v *DeviceSecurity* službách na implementovanie kontroly prístupu. Tím vývojárov identifikoval špecifické úkony v službách *WLANConfiguration*, *LinkAuthentication* and *RadiusClient*, ktoré sú odporučené ako bezpečné.

**1.3.2 Podpora poverení pre každého klienta**

AP môže mať prostriedky, aby podporoval autentizáciu jednotlivých WLAN klientov s unikátnymi povereniami. Môže to podporovať bez autentizačného serveru pomocou viacerých PSK WPA kľúčov. Alebo, AP môže toto podporovať cez ukazovateľ na autentizačný server, ako je RADIUS server, ktorý je dostupný AP zariadeniu cez premenné, ktoré sú poskytované v *RadiusClient* službe. Alternatívne, AP môže podporovať jednotnú funkcionalitu autentizačného serveru a poskytovať to ako službu UPnP™, špecifikovanú LinkAuthentication službou. Toto je nepovinná služba, ktorá sa môže použiť s AP DCP na podporu autentizácie každého klienta s jednotným autentizačným serverom.

**2. Definície zariadenia**

**2.1 Typ zariadenia**

Nasledujúci typ zariadenia identifikuje zariadenie, ktoré vyhovuje tejto šablóne:

*urn:schemas-upnp-org:device:WLANAccessPointDevice:1*

**2.2 Model zariadenia**

Odporúča sa, aby *WLANAccessPointDevice* bolo implementované s podporou pre zabezpečenie UPnP™ opatrení. Taktiež sa odporúča, aby zabezpečenie UPnP™ opatrení bolo vytvorené pomocou služby *DeviceSecurity*, ako bolo určené UPnP™ bezpečnostnou pracovnou skupinou. Ak je implementovaná, služba *DeviceSecurity* musí obsahovať buď implementáciu v danom zariadení *WLANAccessPointDevice,* alebo v zariadení, ktoré zahrňuje *WLANAccessPointDevice*. Tieto dva modely sú popísané nižšie.

**2.2.1.Popis požiadaviek na zariadenie**

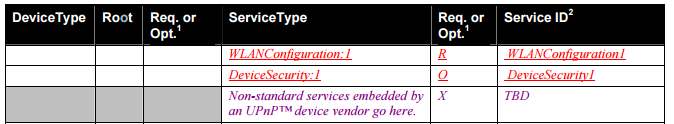
Nasledujúca tabuľka stručne popisuje účel služieb, použitých vo *WLANAccessPointDevice*.

|  |  |
| --- | --- |
| **Názov zariadenia** | **Popis služby** |
| *WLANConfiguration* | Konfiguračné parametre spojené s WLAN odkazom, ktorý musí byť dostupný programovateľne. |
| *DeviceSecurity* | Úkony na prebratie vlastníctva, konfigurácia kontroly prístupu, nastavenie bezpečnostných relácií a vyvolanie bezpečnostných opatrení. |

**2.2.1.1. *DeviceSecurity* v rámci *WLANAccessPointDevice***

Tento model je typicky aplikovateľný na fyzické zariadenia, ktoré potrebujú *DeviceSecurity* funkčnosť (zahrňujúc vlastníctvo zariadenia a kontrolu prístupu), aby mohlo byť použité len zariadením *WLANAccessPointDevice*. V tomto prípade produkty, ktoré vystavujú zariadenia typu *urn:schemas-upnp-org:device: WLANAccessPointDevice:1* musia implementovať minimálny počet verzií služieb, ktoré sú špecifikované tabuľkou nižšie.

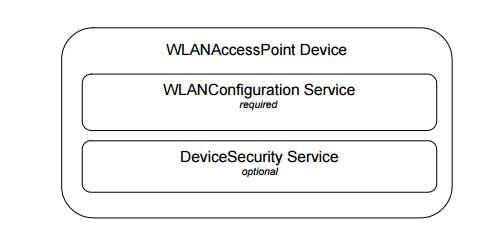
Tabuľka 1: Systémové požiadavky na samostatné zariadenie *WLANAccessPointDevice*



1 R = požadované, O = voliteľné, X = neštandardné  
2 S predponou *urn:upnp-org:serviceId:* .

**Vzťahy medzi službami**

Obrázok 3 znázorňuje logickú štruktúru zariadenia a služieb, definovanú tímom vývojárov pre UPnP™ technológiu, sprístupnenú AP zariadeniam.



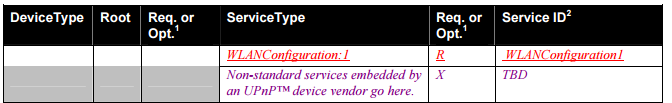
**Obrázok 3: *DeviceSecurity* v rámci zariadenia *WLANAccessPointDevice***

Navyše, služba *LinkAuthentication* (voliteľná) môže byť použitá, ak AP podporuje autentizáciu každého klienta s jednotným autentizačným serverom. *LinkAuthentication, RadiusClient* a*WLANConfiguration* služby môžu byť závislé na službe *DeviceSecurity*, keďže poskytuje kontrolu prístupu k úkonom, ktoré sú definované v daných službách.

**2.2.1.2 *DeviceSecurity* mimo *WLANAccessPointDevice***

Tento model je typicky aplikovateľný na fyzické zariadenia, ktoré implementujú funkcionalitu AP, ale zariadenie *WLANAccessPointDevice* smie použiť *DeviceSecurity*, ktoré je už súčasťou iného zariadenia. Príkladom tohto by mohlo byť zariadenie, kde *urn:schemas-upnp-org:device: WLANAccessPointDevice:1* je implementované v rámci zariadenia typu *urn:schemas-upnp-org:device: BasicDevice:1*. Zariadenie *BasicDevice* v tomto prípade obsahuje službu *DeviceSecurity*, ktorá môže byť použitá iným UPnP™ zariadením, napríklad IGD. Implementácia *WLANAccessPointDevice* musí obsahovať minimálny počet verzií služieb, ktoré sú špecifikované v tabuľke nižšie.

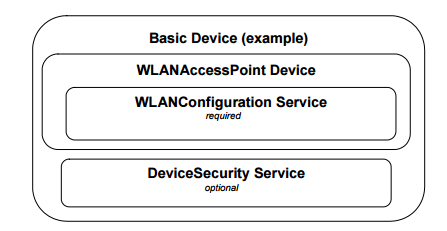
**Tabuľka 2: Systémové požiadavky pre zabudované zariadenie *WLANAccessPointDevice***



1 R = požadované, O = voliteľné, X = neštandardné.  
2 S predponou *urn:upnp-org:serviceId:* .

**Vzťahy medzi službami**

Obrázok 4 zobrazuje logickú štruktúru zariadenia a služieb, definovanú tímom vývojárov pre UPnP™ technológiu sprístupnenú AP zariadeniam, ktoré môžu používať *DeviceSecurity* službu pre ostatné UPnP™ zariadenia v rámci toho istého fyzického zariadenia. Navyše, voliteľná služba *LinkAuthentication* môže byť použitá, ak AP podporuje autentizáciu každého klienta s jednotným autentizačným serverom. *LinkAuthentication, RadiusClient* a*WLANConfiguration* služby môžu byť závislé na službe *DeviceSecurity*, keďže poskytuje kontrolu prístupu k úkonom, ktoré sú definované v daných službách.



**Obrázok 4: Príklad *DeviceSecurity* zariadenia mimo zariadenia *WLANAccessPointDevice***

**2.2.2. Vzťahy medzi službami**

Závislosti medzi službami sú už hore uvedené pod možnými modelmi, ktoré implementujú služby *WLANAccessPointDevice*.

**2.3. Teória fungovania**

Popisuje všeobecný model použitia služieb, definovaných v AP zariadení. Táto sekcia začína zoznamom požiadaviek a voliteľných funkcií WLAN uzlov. Nasleduje sekcia, popisujúca rôzne scenáre použitia týchto funkcií. Pre každú z nich sú špeciálne zdôraznené výhody, umožnené vďaka UPnP™ službám.

Odporúča sa pre AP DCP používať služby *DeviceSecurity*, aby sa dosiahli špecifické UPnP™ AP úkony. Táto sekcia predpokladá celkové porozumenie UPnP™ Security konceptom.

**2.3.1. Požiadavky na WLAN uzly**

Čo sa týka požiadaviek, uzly WLAN spadajú do dvoch kategórií – AP a bezdrôtový používateľ (stanica) AP zariadenia.

**2.3.1.1. AP Požiadavky**

Požiadavky pre 802.11 AP sú uvedené nižšie aj s niektorými voliteľnými funkciami.

* AP musí byť adresovateľný cez IP (Internet Protocol) použitím buď drôtového, alebo bezdrôtového rozhrania. AP funkcionalita sa môže nachádzať na rovnakom mieste ako funkcionalita routera/UPnP™ Internet Gateway Device (IGD) zariadenia a/alebo modemu pre Internetový prístup.
* AP musí poskytovať užívateľovi možnosť fyzicky resetovať zariadenie do pôvodného (výrobného) stavu.
* AP musí podporovať Wireless Protected Access (WPA) v režime PSK (pre-shared key). Musí podporovať aspoň desať PSK kľúčov.
* AP môže implementovať *DeviceSecurity* službu, definovanú v *SecureDevice* Device Control Protocol-e v1.0. Toto zahŕňa použitie páru verejný-súkromný kľúč a kryptografickej knižnice pre autentizáciu a šifrovanie.
* AP môže podporovať 802.1x cez RADIUS klienta (RFC2865, IETF) použitím služby *RadiusClient* UPnP™.
* AP môže podporovať 802.1x cez *LinkAuthentication* službu.

Nepožaduje sa, aby AP mal v základnom nastavení spustenú bezpečnosť odkazu.

**2.3.1.2. Klientske požiadavky na AP konfiguráciu**

Ak je požadovaná konfigurácia AP parametrov, tak musí byť aspoň jeden klient v sieti LAN, ktorý má interaktívne užívateľské rozhranie. Ostatným WLAN klientom môže byť umožnené používať UPnP™ technológiu a vykonávať UPnP™ Control Point funkcionalitu na posielanie úkonov AP zariadeniu. Od všetkých bezdrôtových klientov sa vyžaduje, aby mali rovnaký mechanizmus odkazu bezpečnosti, ktorý používa AP (napríklad 802.1x). WLAN klient musí podporovať aspoň WEP.

**2.3.2. Scenáre predstavenia WLAN klientov AP zariadeniu**

K jednoduchej konfigurovateľnosti AP parametrov, ktoré sú detailnejšie rozobrané v *WLANConfiguration* službe, AP DCP taktiež poskytuje bežný rámec pre schválené zabezpečenie dostatku miesta pre diferenciáciu predajcu. Nasledujúce sekcie popisujú rôzne možné scenáre, keď sa WLAN klient po prvýkrát stretne s AP zariadením a rolou UPnP™ technológie.

**2.3.3. Nastavenie bezpečnostného kontrolného bodu (ak DeviceSecurity je implementované v AP zariadení)**

*WLANConfiguration* služba poskytuje množinu úkonov na modifikáciu a dopytovanie množiny parametrov 802.11 AP zariadenia. Úkony v tejto službe, ktoré modifikujú parametre, by mali byť autentizované cez UPnP™ bezpečnosť. Kontrolný bod, ktorý sprístupňuje bezpečnostné úkony službe, musí byť najskôr autentizovaný cez aplikáciu Security Console, ako je uvedené v UPnP™ Security DCP.

Po zapnutí AP by mal užívateľ spustiť "AP aplikáciu" (kontrolný bod) v klientovi na získanie práv AP zariadenia podľa UPnP™ Security protokolu. Získaním práv tento klient získa autoritu povoľovať, aby špecifické kontrolné body konfigurovali AP, napríklad vloženie bezpečnostných parametrov, zapnutie ochrany, prepnutie do opakovacieho módu, atď.

V prípade, že aplikácia Security Console nebola prístupná od začiatku, AP funguje v základnom nastavení, bez akejkoľvek konfigurácie možnej prostredníctvom UPnP™ technológie.

**2.3.4. AP používa celosieťové poverenia na autentizáciu**

AP využíva zdieľané (pre-shared) celosieťové poverenie špecifikované vo WPA pre všetkých klientov, alebo používa model autentizácie WEP-only .

**2.3.4.1. Počiatočná konfigurácia AP**

"AP aplikácia" konfiguruje zdieľaný kľúč v AP a povoľuje WEP alebo WPA bezpečnosť. Ak "AP aplikácia" je WLAN klientom, musí obnoviť odkaz na AP zariadenie po tom, čo je bezpečnosť odkazu stanovená použitím nového kľúča.

**Prínosy a predpoklady použitia UPnP™ technológie:**  
UPnP™ technológia poskytuje jednoduché nájdenie a konfiguráciu AP zariadenia cez štandardizované programové rozhranie. S AP, ktoré nepodporuje technológiu UPnP™, užívateľ musí zadať URL na web server AP zariadenia a zadať zdieľaný kľúč. Zdieľaný kľúč by mal byť veľmi dlhý, aby bol dostatočne bezpečný, obzvlášť keď sa ním dá ľahko dostať na web server AP zariadenia. Užívateľ musí vedieť o WEP a WPA kľúči a zadávať ho cez prehliadač.

**2.3.4.2. Registrácia nasledujúcich klientov**

Ak AP využíva WPA PSK alebo WEP pre celosieťovú autentizáciu, potom tu neprebieha žiadna   
per-client autentizácia a taktiež ani žiadna potreba *LinkAuthentication* služby, RadiusClient služby alebo akéhoľvek iného autentizačného serveru, ako RADIUS v sieti WLAN. Ak klientske zariadenie má UI (užívateľské rozhranie), užívateľ zadá zdieľaný kľúč (WEP alebo WPA PSK) a dostane odkaz na prístup k AP. Ak klientske zariadenie nemá UI, malo by byť predprogramované s jedinečným kľúčom, ktorý je sprístupnený užívateľovi, napríklad cez nálepku na spodku zariadenia. Užívateľ zadá tento zdieľaný kľúč do AP použitím Control Point aplikácie. Počet takýchto zariadení, ktoré môžu byť pridané je limitovaný počtom zdieľaných kľúčov podporovaných AP zariadením. V prípade WEP je možné pridať štyri zariadenia, a s WPA PSK to bude minimálne desať zariadení, ktoré môžeme pridať.

Alternatívny mechanizmus pre klientov využívajúcich UPnP™ technológiu je, aby klientske zariadenie bolo priamo pripojené (napr. cez Ethernetový kábel) do AP. Klient spustí UPnP™ kontrolný bod a získa zdieľaný kľúč, nakonfiguruje sa a je pripravený k pripojeniu do siete WLAN.

**Prínosy a predpoklady použitia UPnP™ technológie:**Jednoduchý mechanizmus pre pridávanie nových klientov bez UI do AP, ktorý podporuje celosieťové zdieľané kľúče. Alternatívny mechanizmus, spomenutý vyššie, poskytuje spôsob ako pridať klienta bez toho, aby užívateľ zadával kľúč, predpokladá, že klient implementuje UPnP™ Control Point funkcionalitu. Takisto predpokladá, že klient poskytuje drôtové rozhranie pre registráciu, ktoré rozširuje bezdrôtové možnosti. S AP, ktorý neumožňuje UPnP™ technológiu, WLAN klienti nemajú bežný mechanizmus na prístup k bezpečnostným parametrom AP.

**2.3.5. AP používa poverenia "client-specific" na autentizáciu**

Ak AP implementuje autentizačný mechanizmus (napr. 802.1x), ktorý používa rôzne autentizačné poverenia pre každého klienta, autentizačná databáza je použitá na ukladanie a obnovovanie týchto poverení. Autentizačná databáza môže, ale nemusí sa nachádzať v AP. Ak je udržovaný v rámci AP zariadenia, tak potom *LinkAuthentication* služba poskytuje rozhranie k tejto databáze. *LinkAuthentication* služba poskytuje úkony, ktoré umožňujú novému klientovi sa registrovať do siete WLAN. Táto databáza je konzultovaná autentizačným systémom AP na validáciu klienta, ktorý chce nastaviť bezpečnosť odkazu AP zariadeniu. Ak AP používa externý autentizačný server, napríklad RADIUS, tak AP by mal byť nakonfigurovaný adresami, portami a utajenými spôsobmi, ako pristupovať k týmto serverom pomocou úkonov, ktoré sú poskytnuté v *RadiusClient* službe.

**2.3.5.1. Počiatočná konfigurácia AP**

Ak AP používa externý autentizačný server, "control point" aplikácia nastaví informácie o autentizačných serveroch (ako sú IP adresy, port, atď.) v službe *RadiusClient* cez UPnP™ technológiu. Vstup, prislúchajúci tomuto klientovi bude musieť byť pridaný do externého autentizačného serveru (mimo skupinu) pred zavedením ochrany odkazu. Ak je použitý autentizačný server v rámci zariadenia, závislý na implementácii kontrolného bodu, tak potom tento server môže vytvoriť vstup príslušný k tomuto klientovi spolu s povolením v *LinkAuthentication* službe cez UPnP™ technológiu.

**Prínosy a predpoklady použitia UPnP™ technológie:**WLAN klient môže využiť programovú konfiguráciu bezdrôtového rozhrania AP (vrátane umožnenia bezpečnosti odkazu v AP); za predpokladu, že klient implementuje UPnP™ Control Point funkcionalitu, nepotrebuje drôtové rozhranie navyše k bezdrôtovému rozhraniu. S AP, ktorý nepovoľuje UPnP™ technológiu, neexistuje jednoduchá metóda pridania vstupu pre prvého klienta alebo parametrov súvisiacich s autentizáciou do AP zariadenia.

**2.3.5.2. Registrácia nasledujúcich klientov**

Ak AP podporuje autentizačný server v rámci zariadenia, tak UPnP™ Control Point aplikácia je použitá na registrovanie nových klientov do zabezpečenej siete WLAN. Nový klient, ktorý sa pokúsi autentizovať cez AP nie je povinný mať interaktívne užívateľské rozhranie alebo sprístupnenú UPnP™ technológiu. Predpokladá sa, že tento klient podporuje autentizačnú metódu, ktorú požaduje AP zariadenie, pre bezpečnosť odkazu (napr. 802.1x). Mechanizmus používa voliteľnú *LinkAuthentication* službu a proces registrácie je popísaný v dokumente služby *LinkAuthentication*.

Ak je autentizačný server mimo AP, potom externý mechanizmus (iný ako mechanizmy UPnP™ technológie) je použitý na obnovenie databázy, ktorá je používaná týmto autentizačným serverom, za účelom pridania vstupu príslušnému novému klientovi.

V oboch prípadoch sa predpokladá, že WLAN klient má možnosť autentizovať AP zariadenie počas registrácie a následnej autentizácie.

**Prínosy a predpoklady použitia UPnP™ technológie:**  
V situácii, kde autentizačný server je v rámci zariadenia, použitie *LinkAuthentication* služby v AP zjednodušuje administratívu autentizácie 802.1x a robí ju viac použiteľnú v domácom prostredí. Nový WLAN klient môže byť registrovaný do zabezpečenej siete WLAN použitím Control Point aplikácie. *LinkAuthentication* služba poskytuje bežné rozhranie na modifikáciu 802.1x autentizačnej databázy.

Ak autentizačný server je mimo AP zariadenia, voliteľná *RadiusClient* služba poskytuje potrebné premenné a úkony pre akýkoľvek program na konfiguráciu AP s informáciou o autentizačnom serveri/ serveroch. Predpokladá sa tu, že je tu klient v sieti, ktorý implementuje UPnP™ Control Point a poskytuje užívateľské rozhranie; nový WLAN klient nepotrebuje drôtové rozhranie navyše k bezdrôtovému rozhraniu.

**3. XML popis zariadenia**

<?xml version="1.0"?>

<**root** xmlns="urn:**schemas-upnp-org**:**device-1-0**">

<**specVersion**>

<**major**>1</**major**>

<**minor**>0</**minor**>

</**specVersion**>

<**URLBase**>*base URL for all relative URLs*</**URLBase**>

<**device**>

<**deviceType**>urn:**schemas-upnporg**:**device**:WLANAccessPointDevice:1</**deviceType**>

<**friendlyName**>*short user-friendly title*</**friendlyName**>

<**manufacturer**>*manufacturer name*</**manufacturer**>

<**manufacturerURL**>*URL to manufacturer site*</**manufacturerURL**>

<**modelDescription**>*long user-friendly title*</**modelDescription**>

<**modelName**>*model name*</**modelName**>

<**modelNumber**>*model number*</**modelNumber**>

<**modelURL**>*URL to model site*</**modelURL**>

<**serialNumber**>*manufacturer's serial number*</**serialNumber**>

<**UDN**>*uuid:UUID*</**UDN**>

<**UPC**>*Universal Product Code*</**UPC**>

<**iconList**>

<**icon**>

<**mimetype**>**image***/format*</**mimetype**>

<**width**>*horizontal pixels*</**width**>

<**height**>*vertical pixels*</**height**>

<**depth**>*color depth*</**depth**>  
 <**url**>*URL to icon*</**url**>

</**icon**>

<!-- *XML to declare other icons, if any, go here* -->

</**iconList**>

<**serviceList**>

<**service**>

<**serviceType**>urn:**schemas-upnporg**:**service**:WLANConfiguration:1</**serviceType**>

<**serviceId**>urn:**upnp-org**:**serviceId**: WLANConfiguration1</**serviceId**>

<**SCPDURL**>*URL to service description*</**SCPDURL**>

<**controlURL**>*URL for control*</**controlURL**>

<**eventSubURL**>*URL for eventing*</**eventSubURL**>

</**service**>

<!-- *Declarations for other services added by UPnP™ vendor (if any) go here* -->

</**serviceList**>

<**deviceList**>

*Description of embedded devices added by UPnP™ vendor (if any) go here*

</**deviceList**>

<**presentationURL**>*URL for presentation*</**presentationURL**>

</**device**>

</**root**>

**4. Dodatok 1: Definície prístupu kontroly (ak služba *DeviceSecurity* je implementovaná)**

Táto sekcia špecifikuje oprávnenia, profily a ACL (Access Control List) vstupu, ktorý sa implementuje v službe *DeviceSecurity*, ktorá dobrovoľne môže byť použitá zariadením *WLANAccessPointDevice*. Toto sa používa službou Security Console na priradenie prístupu kontroly k zabezpečeným úkonom AP zariadeniu na kontrolu dôležitých aplikácií.

**4.1. Oprávnenia**

Nasledujúce oprávnenia sa musia definovať, aby bol udelený prístup kontroly zabezpečených úkonov k službám, ktoré sú zabudované v AP zariadení. Toto sa použije v službách *LinkAuthentication* a *RadiusClient*, ak sú zahrnuté v implementácii AP zariadenia. Oprávnenie musí byť implementované v nasledujúcom XML formáte :

<Permission>

<UIname>APControl</UIname>

<ACLEntry>

<APWG:APDeviceAll/>

</ACLEntry>

<FullDescriptionURL></FullDescriptionURL>

<ShortDescription>

Toto oprávnenie povoľuje kontrolnému bodu nastaviť a získať všetky zabezpečené úkony všetkých služieb AP zariadenia.

</ShortDescription>

</Permission>

XML tágy elementov UIname, ACLEntry, FullDescription, ShortDescription a Permission sú definované v špecifikáciách služby *DeviceSecurity 1.0*.

Vyššie uvedené oprávnenie má byť vrátené AP zariadením v “DefinedPermissions” argumente, pomocou funkcie GetDefinedPermission v *DeviceSecurity*. Je možné, že obchodníci môžu definovať dodatočnú množinu oprávnení pre kontrolu prístupu k AP zariadeniu. Napríklad, môžu poskytovať separátne oprávnenia (admin a užívateľ) pre ďalšiu členitosť prístupu.

Ak *DeviceSecurity* služba sa nachádza v rámci zariadenia *WLANAccessPointDevice*, tak bude obsahovať iba definované oprávnenia AP zariadenia (ako je uvedené nižšie). Argument “DefinedPermissions”, ktorý vracia služba *DeviceSecurity* funkciou GetDefinedPermission bude :

<DefinedPermissions>

<Permission>

<UIname>APControl</UIname>

<ACLEntry>

<APWG:APDeviceAll/>

</ACLEntry>

<FullDescriptionURL></FullDescriptionURL>

<ShortDescription>

Povoľuje tejto aplikácii kompletnú kontrolu bezdrôtového AP.

</ShortDescription>

</Permission>

</DefinedPermissions>

Ak *DeviceSecurity* služba sa nachádza mimo zariadenia *WLANAccessPointDevice* a *WLANAccessPointDevice* je zabudované v rámci obaľovacieho zariadenia (kontajner) s inými zariadeniami ako sú IGD, tak potom argument “DefinedPermissions”, ktorý vracia služba *DeviceSecurity* funkciou GetDefinedPermission bude :

DefinedPermissions>

<Permission>

<UIname>APControl</UIname>

<ACLEntry>

<APWG:APDeviceAll/>

</ACLEntry>

<FullDescriptionURL></FullDescriptionURL>

<ShortDescription>

Povoľuje tejto aplikácii kompletnú kontrolu bezdrôtového AP.  
</ShortDescription>

</Permission>

<Permission>

napr. oprávnenie definované IGD zariadením.

</Permission>

…

</DefinedPermissions>

**4.2. Profily**

Žiaden profil nie je špecifikovaný na používanie AP zariadením. Obchodníci však môžu definovať svoje profily.

**4.3. Vstup ACL (Acces Control List)**

Ak je služba DeviceSecurity implementovaná v UPnP™ AP zariadení, *WLANAccessPointDevice* má iba

“<APWG:APDeviceAll>” definované oprávnenie pre kontrolu prístupu. Nasledujúce XML zobrazuje príklad ACL vstupu, ktorý umožňuje toto definované oprávnenie kontrolnému bodu špecifikovanému v podelemente. Reťazcová hodnota “dRDPBgZz…” pod tágom <hash> označuje hash kontrolného bodu verejného kľúča, pre ktorý je tento ACL definovaný nasledovne:

<acl>

<entry>

<subject>

<hash>

<algorithm>SHA1</algorithm>

<value>dRDPBgZzTFq7Jl2Q2N/YNghcfj8=</value>

</hash>

</subject>

<access>

<APWG:APDeviceAll/>

</access>

<valid>

<not-before>2001-10-23\_05:17:32</not-before>

<not-after>2003-12-31\_23:59:59</not-after>

</valid>

</entry>

</acl>