Komunikacijski izzivi platforme Tuya Smart v pametnem domu

Andrej Štern

Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška 25, 1000 Ljubljana
E-pošta: andrej.stern@fe.uni-lj.si

Communication challenges of the Tuya Smart platform in a smart home

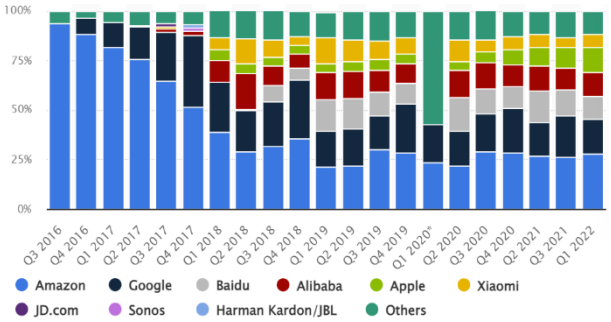
Abstract. *Smart home solutions encompass dedicated devices integrated for capturing and processing data, making decisions, and controlling target units. This paper focuses on the Tuya Smart platform, which offers a comprehensive ecosystem for connecting and managing smart home devices. The study analyzes the communication between Wi-Fi-based Tuya devices and the Tuya Smart platform. Traffic patterns of a smart plug, a smart bulb, and a web camera are examined, revealing communication protocols, addresses, and traffic volume. The findings contribute to understanding the information security and privacy implications of using Tuya devices in a smart home environment.*

1 Uvod

Avtomatizacija upravljanja pametnega doma obsega sklop namenskih naprav, logično združenih v sistemu za zajem, procesiranje, odločanje in upravljanje ciljnih enot. Izraz »pametno« tako ne izvira iz posamezne priključene naprave, temveč iz celotnega sistema s številnimi možnostmi nastavitev čez upravljavski vmesnik na telefonu ali namenskih stenskih zaslonih. Najvišjo stopnjo pameti bi predstavljal sistem, ki bi po začetni vzpostavitvi avtonomno deloval in se prilagajal uporabnikom brez dodatnih posegov v nastavitve.

Prvi pomemben korak k enostavnosti uporabe predstavljajo sistemi glasovnega upravljanja, kot so npr. Google Home z Google Assistant in zvočniki Nest, Amazon Alexa z zvočniki Amazon Echo ter Apple Homekit z družinami naprav HomePod in iPhone z govorno asistentko Siri. Slika 1 prikazuje spreminjanje njihovih tržnih deležev po letih [1]. Zgolj pametni zvočniki z govorno interakcijo so zadostni za npr. iskanje informacij po spletu in branje novic ter elektronske pošte, za nastavljanje osvetlitve, nadzor temperature in proženje alarmov glede vhodnih veličin pa potrebujemo še dodatne naprave, ki tipajo okolje, sprejemajo ukaze in jih pretvarjajo v fizično ali logično aktivnost.

Ključne namenske naprave v pametni hiši lahko po vlogah razdelimo v več kategorij. Senzorji okolja, npr. merilniki temperature in vlage, prispevajo podatke z neko periodo, delujejo enosmerno proti centralnemu sistemu in ne omogočajo odzivnega ravnanja. Alarmni senzorji, npr. detektorji izliva vode, gibanja v prostoru ali odprtih vrat, prispevajo podatke le v primeru doseženih meja, njihova avtonomnost ob baterijskem delovanju pa lahko znatno preseže senzorje s stalno periodo pošiljanja.



Slika 1. Gibanje tržnih deležev akterjev na področju glasovnih storitev pametnega doma v letih 2016 - 2022

Ustrezno povratno ravnanje je doseženo z različnimi aktuatorji, upravljanimi s strani centralne logike, npr. stikala, pogoni senčil, krmilniki ventilov in elektronske ključavnice. Med ne-mehanske aktuatorje lahko štejemo še IR-oddajnike za upravljanje obstoječih ne-pametnih naprav, sisteme za nastavljivo ambientalno osvetlitev z barvnim spektrom RGB in radijske oddajnike, ki nadomeščajo fizične pritiske obstoječih upravljalnikov. Zadnja večja skupina so večpredstavnostne naprave, ki lahko delujejo kot vhodi in/ali izhodi, npr. pametne kamere za zajem slike in zaznavo gibanja s sledenjem osebi, domofoni z video prenosom in dvosmerno govorno komunikacijo ipd.

Pri vzpostavitvi pametnega okolja v hiši želimo doseči čim večjo neodvisnost od proizvajalcev opreme. Razlogi za to so različne izvedbe pametnih naprav, saj ponudniki sistemov, tudi Google, Amazon in Apple, ne ponujajo celotnega spektra funkcionalnosti. Zato večina ponudnikov pametnih naprav omogoča poleg delovanja v lastnem oblaku tudi integracijo z omenjenimi znanimi akterji z glasovnimi rešitvami. Med bolj znanimi rešitvami modularne opreme so izdelki Sonoff podjetja Itead Studio, Shelly podjetja Allterco, Xiaomi Mi Home istoimenskega podjetja, Philips Hue za področje osvetlitev in tudi izdelki Tuya partnerjev z izrazito širokim naborom naprav.

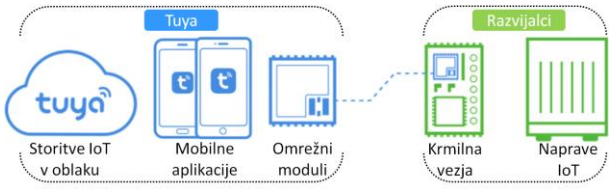
Pri vzpostavitvi domače arhitekture je potrebno premisliti tudi o povezljivosti v oblak oz. zgolj lokalnem delovanju. Uporaba oblaka, značilna za rešitve velikih podjetij, prinaša številne prednosti in tudi slabosti. Med prednostmi prevladujejo bolj preprosta vzpostavitev brez potrebnega tehnološkega predznanja, prilagodljivost upravljanja doma prek pametnih povezanih naprav od kjerkoli na svetu, lažje dodajanje in spreminjanje delovanja naprav brez pomembnih sprememb strojne opreme ali infrastrukture zaradi shranjevanja v oblaku, povezljivost z drugimi spletnimi ali oblačnimi sistemi, možnosti samodejnih posodobitev z najnovejšimi

funkcijami in izboljšavami varnosti ter druge. Med slabostmi sistemov v oblaku prednjačijo odvisnost delovanja rešitve od internetne povezave, pomisleki glede zasebnosti in varnosti, kar zahteva slepo zaupanje v delovanje sistema nekje na svetu, potencialni stroški naročnine za dostop do naprednih funkcij ali mesečni pavšal ter odvisnost od ponudnika storitev, ki lahko doživi tehnične težave ali se celo odloči, da prekine s ponudbo dela storitev ali s podporo določenim napravam. Tako so znani primeri, ko je ponudnik Sonos z uvedbo nove generacije leta 2019 prekinil delovanje starejših zvočnikov s popustom za nakup novih, v letu 2023 pa je Xiaomi odrekel zelo oglaševano shranjevanje video posnetkov s kamer v oblaku za zadnjih 7 dni za trge izven Kitajske in Indije. Nasprotno, lokalne namestitve brez oblaka omogočajo več nadzora nad vzpostavljeno infrastrukturo, svobodo prilagajanja in spreminjanja sistema glede na dejanske potrebe, dobro delovanje tudi brez internetne povezave ter povečano zasebnost in varnost rešitev. To zahteva večje vložke v izgradnjo sistema in več tehničnega znanja za npr. vzpostavitev in upravljanje lastnih strežnikov, ročna posodabljanja sistema ter integracijo z zunanjimi ponudniki storitev. Priljubljeni predstavniki lokalnih rešitev so Home Assistant, ESPhome, OpenHAB in Domoticz, ki ponujajo tudi integracijo z drugimi sistemi v oblaku.

Prispevek predstavlja analizo omrežnega prometa naprav Tuya v domačem okolju z namenom določitve izzivov varnosti in zasebnosti pri komunikaciji v oblak.

2 Platforma Tuya Smart

Kitajsko podjetje Tuya se je po ustanovitvi leta 2014 osredotočalo na programski razvoj platforme za povezovanje in upravljanje pametnih naprav prek enotnega vmesnika. Kmalu so predstavili platformo Tuya Smart za pametne domove, ki združuje koncepta platforme kot storitve PaaS (angl. Platform as a Service) in programske opreme kot storitve SaaS (angl. Software as a Service). Slika 2 [2] prikazuje skupek storitvene platforme, strojne in programske opreme, ki je na voljo razvijalcem storitev.



Slika 2. Tuya ekosistem za preprost razvoj rešitev IoT

V letu 2023 je v platformo Tuya, kjer se zagotavlja storitve IoT za okoli 8000 podjetij, prijavljenih 800.000 razvijalcev iz 200 držav [3]. Predstavniki podjetja Tuya delujejo v Zavezništvu za standarde povezljivosti CSA (angl. Connectivity Standards Alliance), kjer podpirajo novejši protokol za IoT Matter in sodelujejo z velikimi korporacijami, kot so Philips, Schneider Electric in Lenovo. Tako je Tuya danes povsem globalno podjetje, ki kotira tudi na borzah NYSE: TUYA in HKEX: 2391.

Arhitektura Tuya Smart je za zagotavljanje večje kapacitete in nižjih odzivnih časov razdeljena na 6 svetovnih regij: na Kitajsko, vzhod ZDA, zahod ZDA, srednjo Evropo, zahodno Evropo in Indijo. Regija se uporabnikom avtomatsko določi ob registraciji mobilne aplikacije in je kasneje ni možno preprosto spremeniti, saj so uporabniški podatki shranjeni le v regionalnem podatkovnem centru, kjer velja lokalna zakonodaja o ravnanju s podatki. Slovenijo pokriva centralno-evropski center v Frankfurtu, Nemčija, vzpostavljen v oblaku Amazon AWS (angl. Amazon Web Services). Prehajanje med regijami, npr. klici API v drug podatkovni center, niso dovoljeni, kar lahko povzroča težave pri integraciji Tuya naprav z drugimi sorodnimi sistemi (npr. Home Automation). Poleg AWS uporabljajo druge regije tudi gostovanje pri Microsoft Azure (zahodna Evropa, vzhodna Amerika) in v oblaku Tencent (Kitajska). Vsak dan ti centri iz pametnih naprav po svetu zberejo in obdelajo prek 100 milijonov podatkov in zahtev [2].

Del ekosistema predstavlja nabor Tuya omrežnih modulov za pokrivanje različnih potreb pri razvoju in zagotavljanju storitev IoT. V grobem se delijo po komunikacijskem dosegu na lokalno (LAN) in širše (WAN) pokrivanje. Med lokalne dosege spadajo Bluetooth, ZigBee in Wi-Fi ter komunikacije na 433 in 868 MHz, med širše pa mobilni GPRS ter namenski IoT tehnologiji NB-IoT in LTE Cat.1 [3].

Za module velja posebno označevanje, npr. TYWE3S sestavlja oznaka za splošni namen TY (Tuya Smart), W za Wi-Fi, E za proizvajalca radijskega čipa Espressif, oznaka serije 3 in dodatek S za visoko zmogljivost brez posebej nizke porabe. Ta starejši modul je dejansko osnovan na znanem vezju SoC (angl. System-On-Chip) ESP8266. Novejši moduli LAN vsebujejo jedra proizvajalcev Realtek, Xradiotech, Beken, Nordic, Telink, Silicon Labs in ostalih [3]. Tak komunikacijski modul dejansko služi samo za pokrivanje potreb povezljivosti z zagotavljanjem ustrezne varnosti, zato na njem pri razvoju ni možno izvajati še drugih funkcij, npr. odčitavati senzorje in vklapljati releje. To je precejšnje presenečenje, saj smo razvijalci navajeni, da npr. v ESP8266 vnesemo programsko kodo za komunikacijski in hkrati tudi storitveni del. V primeru Tuye programsko opremo za modul zagotovi sama platforma, od konfiguracije funkcij na razvijalskem portalu [3] pa je odvisno, kaj modul zna. Na spletu je možno najti več podrobnih, a neustreznih starejših navodil, kako s pomočjo ESP8266 in dodatne Arduino plošče registriramo svojo Tuya napravo, žetone za identifikacijo pa pridobimo prek namenske razvijalske elektronske pošte devops@tuya.com. Tak sistem je bil v zadnjih dveh letih preoblikovan v komercialni smeri, ki brezplačen razvoj ponuja le v številčno in časovno omejenem obsegu [4]. Zato so analize prometa pametnih naprav v prispevku potekale zgolj za gotove in kupljene izdelke brez vpogleda v notranjo izvedbo.

3 Analiza komunikacije Wi-Fi pametnih naprav s platformo Tuya Smart

Informacijska varnost platforme Tuya Smart se skupaj s pripadajočimi aplikacijami, pametnimi napravami in storitvami redno preverja s strani tretjih organizacij, za sistem pa se pridobivajo različni certifikati. Povzetek aktivnosti na področju skladnosti in informacijske varnosti za Tuyo Smart je objavljen v t.i. beli knjigi [5], v kateri je podrobno opisana združljivost s standardi in uredbami, npr. z ISO 27001 za upravljanje informacijske varnosti, ISO 27017 za nadzor informacij v oblaku, ISO 27701 za zaščito zasebnosti, CSA STAR za varno okolje računalništva v oblaku, ISO 9001 za vodenje kakovosti, ETSI EN 303645 za kibernetsko varnost, evropsko uredbo GDPR ter drugimi [5]. Še več, za odkrivanje ranljivosti s strani zunanjih uporabnikov je vzpostavljen odzivni center na naslovu https://src.tuya.com/, kamor se lahko javljajo posamezna opažanja. Ko se sporočena ranljivost celovito oceni po tehničnih zahtevah, obsegu vpliva, zahtevnosti odkrivanja, poslovni pomembnosti in morebitni škodi, se prijavitelju lahko izplača denarna nagrada, težava pa bo odpravljena skladno s SLA (angl. Service Level Agreement) glede na stopnjo nujnosti v obdobju od 12 ur do 7 dni [5].

Kljub zagotovilom številnih organizacij o visokih nivojih informacijske varnosti platforme Tuya je vredno tem vidikom nameniti dodatno pozornost, saj govorimo o zasebnem delu našega življenja in tudi o domačem komunikacijskem omrežju, kjer si neželenih gostov ne želimo. Za ta namen je bilo v Laboratoriju za telekomunikacije, UL FE, prek prenosnika vzpostavljeno namensko Wi-Fi omrežje v obliki Wi-Fi dostopne točke, ki je stregla različne Tuya naprave. Omrežju Wi-Fi je tako pripadalo zasebno podomrežje IP z naslovi 192.168.137.0/24, ki se je prek privzetega prehoda usmerjalo v zunanja omrežja proti podatkovnim centrom Tuya. Testna arhitektura za zajem prometa Wi-Fi s programskim orodjem Wireshark je prikazana na sliki 3.

Slika 3. Testna arhitektura za zajem prometa Wi-Fi na vzpostavljeni dostopni točki na prenosniku

Za naprave s komunikacijo Bluetooth in ZigBee (BT/ZB) je bil dodan Tuya komunikacijski prehod, ki BT/ZB komunikacijo prevede na lokalno omrežje IP in naprej proti oblaku. Prednost BT/ZB komunikacij je vsekakor v nižji porabi energije, kar omogoča večjo avtonomnost ob baterijskem napajanju oz. bolj pogosto pošiljanje podatkov v oblak. Če je za posodabljanje temperature prek Wi-Fi primerna perioda 1 h, lahko za doseg iste avtonomnosti z BT/ZB preidemo na minutni nivo. Ker pa BT/ZB komunikacija na omrežnem nivoju ne uporablja protokola IP, v analizi posebej ni bila zajeta in obravnavana.

V meritve in analizo prometa je bilo vključenih več Tuya naprav z vmesnikom Wi-Fi, kot je prikazano na sliki 4: (1) krmiljena vtičnica 220V/20A z možnostjo spremljanja porabe, (2) 220V 15W žarnica z grlom E27 in možnostjo nastavitev različnih scenarijev svetilnosti ter (3) spletna kamera Fuers 1080P s funkcijami sledenja, dvosmerne govorne komunikacije in drugimi.

Slika 4. Naprave Tuya, zajete v analizi Wi-Fi prometa

3.1 Promet pametne vtičnice

Scenarij zajema prometa pametne vtičnice obsega 18 ur neprekinjenih meritev. Večino osrednjega časa naprava s strani mobilne aplikacije ni bila krmiljena, zato so se opazovale aktivnosti predvsem v mirovnem stanju. Na koncu meritev je bilo izvedenih 10 zaporednih daljinskih vklopov in izklopov vtičnice. Ta je bila povezana v omrežje z naslednjimi naslovi:

- IPv4: 192.168.137.119,
- MAC: Espressi_21:d6:32 (48:3f:da:21:d6:32).

Po osnovni priključitvi v omrežje Wi-Fi je naprava naslavljala le tri različne naslove IP, kjer sta bili ugotovljeni 2 mirovni periodi.

Namen prve periode je oglaševanje prisotnosti naprave v lokalnem omrežju na broadcast naslova IP 255.255.255.255 in MAC vsakih 5 sekund. S takim oglaševanjem se nešifrirano, a v binarni obliki, oddajajo bistveni podatki, ki omogočajo prepoznavo naprave, dodajanje v uporabniški vmesnik in njeno upravljanje. Ker je vtičnica neprestano pod napajanjem, oglaševalskih aktivnosti med delovanjem ne prekine.

Druga perioda je namenjena vzdrževanju aktivne seje vsakih 60 s z oblakom AWS v Frankfurtu na naslovu 18.185.218.106 in vratih 8886. Tako vzdrževanje je nujno, saj ukazi iz mobilne aplikacije potujejo v oblak, od tam pa se morajo prenesti do naprav v domačem lokalnem omrežju, ki načeloma iz javnega interneta ni dostopno. Z uporabo t.i. MQTT »keep-alive« mehanizma lahko prek vzpostavljene seje vtičnica posluša ukaze iz oblaka in se hitro odzove. Komunikacija z naslovom 18.185.182.159 se je zgodila le za namene vzpostavljanja varne HTTP povezave (t.i. SSL rokovanje) na vratih 443.

Pri daljinskih vklopih in izklopih vtičnice pride iz oblaka z naslova 18.185.218.106 šifrirana zahteva na ista TCP izvorna vrata, kot so bila vzdrževana vsako minuto, torej iz 8886 nazaj na 38842. Ker vsebina komunikacije zaradi šifriranja TLSv1.2 ni dostopna, lahko opazujemo le klasično izmenjavo podatkov v največ 2 zaporednih zahtevah in odgovorih s končnimi potrditvami.

3.2 Promet pametne žarnice

Scenarij opazovanja prometa pametne žarnice v trajanju 3 ur je zajemal analizo v mirovanju in ob krmiljenju. Naprava je bila prisotna z naslednjimi naslovi:

- IPv4: 192.168.137.237,
- MAC: TuyaSmar_b3:52:dd (38:1f:8d:b3:52:dd).

Po osnovni priključitvi v omrežje Wi-Fi je naprava naslavljala tri različne naslove IP, kjer so bile ugotovljene 3 mirovne periode.

Za odkrivanje naprave v lokalnem omrežju na 255.255.255.255 in vratih 6667 s periodo 5 s veljajo ugotovitve pri pametnem stikalu. Komunikacija z oblakom AWS na 3.121.131.36 se odvija vsakih 1500 s, striktno za namene vzpostavljanja varne HTTP povezave (SSL rokovanje) na vratih 443. V primerjavi s stikalom z le 2-kratnim rokovanjem v 18 h je tu razlika v večji pogostosti in periodičnosti vzpostavljanja.

Vzdrževanje aktivne seje MQTT s podatkovnim centrom EU Central AWS na 18.185.31.196 poteka vsakih 60 s na vratih 8886, v primerjavi s stikalom pa je bil periodični promet tu bolj količinsko raznolik.

Pri krmiljenju žarnice pride z naslova podatkovnega centra zahteva na ista TCP izvorna vrata, kot so bila vzdrževana vsako minuto, torej iz 8886 nazaj na 40107.

3.3 Promet spletne kamere

Spletna kamera je večfunkcijska naprava, ki omogoča prenose videa z dvosmerno govorno zvezo, sproža alarme v primeru doseženih nastavljenih meja in vsebuje zajeten sistem upravljanja. Zaradi obsežnosti in raznolikih komunikacij do oblaka se je skušalo ugotoviti predvsem to, ali kdo dostopa do kamere brez naše vednosti oz. če kdo nastavitev načina zasebnosti, kjer dostop do videa in avdia ni mogoč, zaobide. Tak prenos bi izstopal po količini prometa, kar je s programom Wireshark preprosto ugotoviti. Kamera je bila zato spremljana 26 ur na naslovih:

- IPv4: 192.168.137.152,
- MAC: AltoBeam_8d:8c:e0 (88:28:7d:8d:8c:e0).

Poleg znanega oglaševanja na 5 s kamera izvaja tudi PING na naslove privzetega prehoda in Googlov javni strežnik DNS 8.8.8.8. S tem očitno testira dosegljivost interneta, saj kamera v testu brez zunanje povezave, torej neposredno med aplikacijo na telefonu in kamero na istem omrežju Wi-Fi, ni delovala. Poleg tega vsaki 2 minuti na 239.255.255.250 (multicast naslov v lokalni mreži) pošilja še poizvedbe SSDP (angl. Simple Service Discovery Protocol).

Odgovor na vprašanje o nepooblaščenih vpogledih v video je dala primerjava med načinom mirovanja v dolžini 26 h ter drugo meritvijo, kjer se je video prenašal. V mirovanju kamere znaša največja gostota prometa 30 paketov v sekundi s povprečjem 6, pri prenosu videa pa povprečje okoli 180 z maksimumom prek 500 oddanih paketov v sekundi. Iz opazovanih maksimumov in povprečij prenesenih paketov lahko zaključimo, da v opazovanih 26 urah kamere z vklopljenim načinom zasebnosti poskusov prenosa video signala ni bilo.

4 Sklep

Pametne naprave Tuya lahko v domačem okolju izboljšajo kakovost bivanja, povečajo varnost in zaščito doma ter povečajo pregled nad stanjem, še posebej v primeru naše odsotnosti, npr. na počitnicah ali v službi. Pri pogovorih s kolegi z matične fakultete in drugimi zainteresiranimi skupinami so bili večkrat izpostavljeni izzivi »velikega brata«, še posebej pri uporabi govornih asistentov in video kamer, ki lahko globlje posežejo v našo zasebnost.

Analiza omrežnega prometa s tremi različnimi Tuya napravami je podala vzorec povezljivosti, ki zajema periodično oglaševanje naprave v lokalnem omrežju, vzpostavljanje varne povezave do oblaka in vzdrževanje aktivne seje MQTT z oblakom za prenos izmerjenih veličin in sprejem ukazov s pametnega telefona. Podrobna vsebina na aplikacijskem sloju ni bila analizirana, saj je vsebina šifrirana in do posameznih veličin znotraj podatkovne enote ni možno dostopati. Iz statističnega opazovanja periodičnosti in količine prometa ter uporabe naslovov IP lahko sklepamo, da v času meritev ni bilo zaznanih posebnosti, ki bi kazale na kršenje osnovnih pravil informacijske varnosti. Seveda pa tudi največji opazovani interval 26 ur ni dovolj, da bi lahko to trdili tudi za v bodoče.

Osnovni problem lahko nastane že s posodabljanjem v pametne naprave vgrajene programske opreme, ki izvira s strani platforme Tuya. Zlonamerna programska oprema na pametni napravi lahko v domačem lokalnem omrežju zbira podatke, odkriva ranljivosti omrežja in celo izvaja ciljne množične napade DDoS (angl. Distributed Denial-of-Service) na svetovne strežnike. Zato se priporoča, da vse pametne naprave vključimo v ločeno lokalno podomrežje, od koder do računalnikov in omrežnih diskov nimajo dostopa. Nenazadnje lahko tudi nabor naprav omejimo le na tiste, ki ne morejo kršiti naše zasebnosti (kot npr. kamere), ogroziti varnosti (kot npr. elektronske ključavnice) ali povzročiti škode (kot npr. grelna telesa in razni ventili).

Literatura

[1] Statista: Market share of global smart speaker shipments from 3rd quarter 2016 to 1st quarter 2022, by vendor, junij 2022, https://www.statista.com/statistics/792604/worldwide-smart-speaker-market-share/

[2] Tuya: Tuya IoT Development Platform, julij 2023, https://developer.tuya.com/en/docs/iot/introduction-of-tuya?id=K914joffendwh

[3] Tuya: Network Module, maj 2023, https://developer.tuya.com/en/docs/iot/network-module-overview?id=Ka4z12ojepber

[4] Tuya: Get Free Licences, november 2022, https://developer.tuya.com/en/docs/iot-device-dev/sweep_device_03?id=Kb6jmqyfq1zkp

[5] Tuya: Tuya Smart White Paper on Information Security & Compliance, različica 5.2, leto 2022, https://images.tuyacn.com/smart/docs/TuyaSmart-WhitePaper-Intl.pdf