ETSI TR 102 732 V1.1.1 (2013-09)

Komunikácia stroj-stroj (M2M);
Prípady používania aplikácií M2M v elektronickom zdravotníctve

Machine-to-Machine communications (M2M);
Use cases of M2M applications for eHealth

Európsky inštitút pre telekomunikačné normy

European Telekommunications Standards Institute

Referenčné číslo

DTR/M2M-00005ed111

Kľúčové slová

ageing, emergency, health, interworking,
M2M, use case

ETSI

650 Route des Lucioles
F–06921 Sophia Antipolis Cedex – France

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Neziskové združenie registrované
na podprefektúre de Grasse (06) N° 7803/88

Dôležité upozornenie

Jednotlivé kópie tohto dokumentu možno stiahnuť z

http://pda.etsi.org

Tento dokument môže byť dostupný vo viacerých elektronických verziách alebo v tlačenej forme. V prípade existujúceho alebo viditeľného rozdielu v obsahu medzi takýmito verziami je referenčnou verziou verzia v prenosnom dokumentovom formáte (Portable Document Format – PDF).

V prípade sporu je referenčným výtlačok vytlačený na tlačiarni ETSI z verzie PDF uchovávanej na určenom sieťovom serveri sekretariátu ETSI.

Používatelia tohto dokumentu by mali brať do úvahy, že dokument môže byť revidovaný alebo sa môže zmeniť jeho postavenie. Informácie o postavení tohto dokumentu a ďalších dokumentov ETSI sú dostupné na

http://portal.etsi.org/tb/status/status.asp

Ak nájdete v tomto dokumente chyby, svoje pripomienky zašlite na

http://portal.etsi.org/chaircor/ETSI_support.asp

Obsah

Práva duševného vlastníctva 5

Predhovor 5

1 Predmet 6

2 Referenčné dokumenty 6
2.1 Normatívne referenčné dokumenty 6
2.2 Informatívne referenčné dokumenty 6

3 Definície a skratky 7
3.1 Definície 7
3.1 Skratky 7

4 Aplikácie M2M v elektronickom zdravotníctve 9
4.1 Všeobecný opis aplikácií M2M v elektronickom zdravotníctve 9
4.2 Konkrétne príklady aplikácií M2M v elektronickom zdravotníctve 10
4.2.1 Manažérstvo ochorení 10
4.2.2 Nezávislé starnutie 10
4.2.3 Zlepšovanie fyzickej spôsobilosti osôb a zdravia 11

5 Prípady používania aplikácií M2Mv elektronickom zdravotníctve 12
5.1 Diaľkový dohľad nad pacientom (RPM) 12
5.1.1 Všeobecný opis 12
5.1.2 Zainteresované subjekty 12
5.1.3 Scenár 13
5.1.4 Výmena informácií 14
5.1.5 Potenciálne nové požiadavky 14
5.1.5.1 Inicializácia a registrácia zariadenia 14
5.1.5.2 Komunikácia zariadenia 15
5.1.5.2.1 Diaľkové riadenie a konfigurácia 15
5.1.5.2.2 Telemetria pacienta (vyhľadávanie a distribúcia dát) 17
5.1.5.3 Odvodené potenciálne nové požiadavky 18
5.2 Bezpečné zasielanie správ pacient – poskytovateľ 18
5.2.1 Všeobecný opis 18
5.2.2 Zainteresované subjekty 19
5.2.3 Scenár 20
5.2.3.1 Kategórie a platformy bezpečného zasielania správ 20
5.2.3.1.1 Zariadenie M2M (alebo systém/aplikácia)-zariadenie M2M (alebo systém/aplikácia) 20
5.2.3.1.2 Zariadenie M2M (alebo systém/aplikácia)-používateľ (pacient alebo poskytovateľ) 20
5.2.3.1.3 Používateľ (pacient alebo poskytovateľ)-zariadenie M2M (alebo systém/aplikácia) 20
5.2.3.1.4 Platformy zasielania správ 20
5.2.4 Výmena informácií 20
5.2.4.1 Počiatočné nastavenie bezpečného zasielania správ 20
5.2.4.1.1 Komunikácia iniciovaná používateľom 20
5.2.4.1.2 Komunikácia iniciovaná zariadením 21
5.2.4.2 Komunikácia iniciovaná pacientom 21
5.2.4.2.1 Komunikácia iniciovaná používateľom 21
5.2.4.2.2 Komunikácia iniciovaná zariadením 22
5.2.4.3 Komunikácia iniciovaná poskytovateľom 23
5.2.4.3.1 Komunikácia iniciovaná používateľom 23
5.2.4.3.2 Komunikácia iniciovaná zariadením 23
5.2.4.4 Iná výmena informácií 23
5.2.4.4.1 Smerovanie dát na základe obsahu 23
5.2.4.4.2 Vzájomná spolupráca (dátový formát atď.) 24
5.2.5 Potenciálne nové požiadavky 24
5.2.5.1 Aktualizácia bezpečných protokolov 24
5.2.5.2 Prenositeľnosť pripojenia 24
5.2.5.3 Sledovanie umiestnenia 25

5.2.5.4 Zdôvodnenie....25
5.2.5.5 Vytvorenie (registrácia) spôsobilosti bezpečného zasielania správ....25
5.2.5.5.1 Registrácia zariadenia....25
5.2.5.5.2 Registrácia používateľa....26
5.2.5.6 Prípady používania komunikácie (iniciované pacientom alebo poskytovateľom)....26
5.2.5.6.1 Komunikácia používateľ – zariadenie (inicializované používateľom)....26
5.2.5.6.2 Komunikácia iniciovaná zariadením....27
5.2.5.7 Údržba zariadenia....28
5.2.5.7.1 Aktualizácia softvéru....28
5.3 Meranie signálov tela s veľmi nízkym napätím (MVLBS)....29
5.3.1 Všeobecný opis....29
5.3.2 Zainteresované subjekty....30
5.3.3 Postup....30
5.3.4 Výmena informácií....30
5.3.5 Potenciálne nové požiadavky....30
5.3.5.1 Elektronické zdravotnícke pomôcky bez rušenia....30
5.3.5.2 Indikácia činnosti rádiového vysielania....30
5.3.5.3 Riadenie činnosti rádiového vysielania....30
5.4 Prenos dát pri starostlivosti na diaľku medzi domácnosťou a vzdialeným monitorovacím centrom....30
5.4.1 Všeobecný opis....30
5.4.2 Zainteresované subjekty....31
5.4.3 Scenár....31
5.4.4 Výmeny informácií....32
5.4.5 Potenciálne nové požiadavky....33
História....35

Práva duševného vlastníctva

Práva duševného vlastníctva, ktoré majú alebo môžu mať zásadný význam pre tento dokument, sa mohli oznámiť organizácii ETSI. Informácie o týchto zásadných právach duševného vlastníctva, ak existujú, sú pre členov i nečlenov ETSI verejne dostupné a môžu ich nájsť v dokumente ETSI SR 000 314 s názvom: Práva duševného vlastníctva (IPR). Zásadné alebo potenciálne zásadné práva duševného vlastníctva, oznámené organizácii ETSI vo vzťahu k normám ETSI, možno získať na sekretariáte ETSI. Najnovšie znenie je dostupné na serveri ETSI (http://ipr.etsi.org).

V súlade so svojou politikou v oblasti práv duševného vlastníctva ETSI neskúma ani nevyhľadáva nijaké práva duševného vlastníctva. Neposkytuje ani záruku na iné práva duševného vlastníctva, ktoré sa neuvádzajú v dokumente SR 000 314 (alebo v jeho aktualizovaných vydaniach na serveri ETSI), ktoré sú alebo môžu byť, alebo by sa mohli stať dôležitými pre predkladaný dokument.

Predhovor

Technickú správu (TR) pripravila technická komisia na komunikáciu stroj-stroj (TC M2M) v ETSI.

Obsah technickej správy je informatívny, ale keď sa odvolá na tento dokument, uvádzané definície sa stávajú normatívne, pokiaľ ide o obsah referenčnej TS.

1 Predmet

Dokument zhromažďuje opisy prípadov používania aplikácií elektronického zdravotníctva v kontexte komunikácie stroj-stroj (M2M). Opísané prípady používania aplikácií M2M sa použijú na odvodenie požiadaviek na služby a spôsobilosti funkčnej architektúry uvedenej v ETSI TC M2M.

2 Referenčné dokumenty

Referenčné dokumenty sú špecifické (označené dátumom zverejnenia a/alebo číslom vydania, alebo číslom verzie) alebo nešpecifické. Pre špecifické referenčné dokumenty platí len citovaná verzia. Pre nešpecifické referenčné dokumenty platí len posledná verzia referenčného dokumentu (vrátane zmien).

Referenčné dokumenty, ktoré nie sú uznané ako verejne dostupné na očakávanom mieste, je možné nájsť na webovej adrese http://docbox.etsi.org/Reference.

POZNÁMKA. – Aj keď všetky hypertextové odkazy obsiahnuté v tomto článku platili v čase publikovania, ETSI nemôže zaručiť ich dlhodobú platnosť.

2.1 Normatívne referenčné dokumenty

Uvedené dokumenty sú dôležité na uplatňovanie dokumentu.

Neuvedené.

2.2 Informatívne referenčné dokumenty

Uvedené dokumenty nie sú dôležité na uplatňovanie dokumentu, ale pomáhajú používateľovi v konkrétnej predmetnej oblasti.

[i.1] IEEE 11073: „Health Informatic – Personal health device communication".

[i.2] BS 8521: 2009: „Specification for dual-tone multi-frequency (DTMF) signalling protocol for social alarm systems".

3 Definície a skratky

3.1 Definície

V dokumente sa používajú termíny a definície:

elektronické zdravotníctvo (angl. **eHealth**): generický pojem pre triedu aplikácií, ktoré slúžia na zlepšenie zdravotnej starostlivosti a zdravotníckych služieb prostredníctvom elektronických informácií alebo komunikačných technológií

POZNÁMKA. – Definícia elektronického zdravotníctva v tomto dokumente zahŕňa veľa rôznych aplikácií.

3.1 Skratky

V dokumente sa používajú skratky:

ECG	Electrocardiography	elektrokardiografia
EHR	Electronic Health Record	elektronický zdravotný záznam
EMR	Electronic Medical Record NOTE. – Typically maintained and managed by the provider.	elektronický lekársky záznam POZNÁMKA. – Typicky udržiavaný a spravovaný poskytovateľom.
EMT	Emergency Medical technician	technik zdravotnej záchrannej služby
M2M	Machine-to-Machine NOTE. – Communications.	stroj-stroj POZNÁMKA. – Komunikácie.
MVLBS	Measurement of Very Low Voltage Body Signals	meranie signálov tela s veľmi nízkym napätím
PGP	Pretty Good Privacy NOTE. – Security protocol for email.	Pretty Good Privacy (obchodná značka) POZNÁMKA. – Bezpečnostný protokol v elektronickej pošte.
PHR	Personal Health Record NOTE. – Typically maintained and managed by the patient.	osobný zdravotný záznam POZNÁMKA. – Typicky udržiavaný a spravovaný pacientom.
RMD	Remote Monitoring Device	vzdialené monitorovacie zariadenie
RPM	Remote Patient Monitoring	diaľkové monitorovanie pacienta
SCL	Service Capability Layer	vrstva prvkov služby
TLS	Transport Layer Security protocol NOTE. – Successor to SSL.	protokol na ochranu transportnej vrstvy

		POZNÁMKA. – Nástupca SSL.
WAN	Wide Area Network	rozsiahla počítačová sieť

4 Aplikácie M2M v elektronickom zdravotníctve

4.1 Všeobecný opis aplikácií M2M v elektronickom zdravotníctve

Aplikácie M2M v elektronickom zdravotníctve umožňujú:

- diaľkový dohľad nad zdravím pacienta a informácie o fyzickej spôsobilosti;
- umožnenie spustenia poplachu pri detekcii kritických podmienok;
- v niektorých prípadoch aj diaľkové ovládanie určitých liečebných postupov alebo parametrov.

Na získanie informácií o zdraví alebo o fyzickej spôsobilosti pacienta sa musia použiť vhodné senzory. Z tohto dôvodu pacient alebo sledovaná osoba obvykle nosí jeden alebo viac senzorov, ktoré zaznamenávajú indikátory zdravia a fyzickej spôsobilosti, ako je krvný tlak, telesná teplota, frekvencia tepu, hmotnosť atď. pozri obrázok 1. Pretože zvyčajne tieto senzory musia vyhovovať pri závažných obmedzeniach, ako je tvar a napájanie z batérií, vo väčšine prípadov sa očakáva, že je potrebné zhromaždené údaje postúpiť pomocou určitej technológie krátkeho dosahu zariadeniu, ktoré môže slúžiť ako agregátor zhromaždených informácií a ako sieťový priechod smerom k subjektu v pozadí, o ktorom sa predpokladá, že uchováva a prípadne reaguje na zozbierané údaje. Je tiež možné, že senzory používané na sledovanie parametrov, ktoré sa týkajú zdravotného stavu pacienta, sa nachádzajú niekde v okolí pacienta.

Obrázok 1– Nositeľné senzory

Model agregácie a odovzdávania zhromaždených informácií pomocou zariadenia s funkciou sieťového priechodu sa v ďalšom nazýva model sieťového priechodu. Nositeľné senzory často používajú rádiové spojenie krátkeho dosahu k zariadeniu s funkciou sieťového

priechodu, ktoré má pripojenie k WAN. Napríklad sieťový priechod môže byť pevné zariadenie, ako je PC alebo settopbox, alebo mobilné zariadenie, ako mobilný telefón, alebo samostatné zariadenie zavesené na retiazke s kľúčmi alebo nosené na zápästí alebo krku pacienta. Zariadenie s funkciou sieťového priechodu potom môže poslať údaje o zdravotnom stave na server v pozadí pomocou WAN, kde si ich môžu zobraziť lekári a pacienti.

V iných prípadoch sa nemusí použiť model sieťového priechodu, napríklad ak senzory majú spôsobilosť podporovať spojenie k serveru v pozadí priamo, bez pomoci zariadenia s funkciou sieťového priechodu. Môže sa to použiť pri senzoroch, ktoré majú integrovaný komunikačný modul WAN.

4.2 Konkrétne príklady aplikácií M2M v elektronickom zdravotníctve

4.2.1 Manažérstvo ochorení

Spoločné používanie aplikácií M2M v elektronickom zdravotníctve podporuje diaľkové manažérstvo chorôb pacienta. Proces riadenia chorôb pacienta sa tu nazýva manažérstvo ochorení. Príklady zahŕňajú:

- manažérstvo diabetu (sledovanie hladiny cukru v krvi, regulácia dávkovania inzulínu);
- manažérstvo srdcových arytmií (príkladom je systém Cardionet, ktorý zaznamenáva občasné abnormálne srdcové rytmy a odosiela dáta pomocou WAN na analýzu).

V aplikáciách manažérstva ochorení sa údaje o zdravotnom stave zvyčajne zhromažďujú pomocou jedného alebo viacerých senzorov a posielajú sa na server v pozadí v pravidelných intervaloch. Množstvo dát, ktoré sa majú zhromažďovať a odovzdávať na server za čas a frekvencia podávania správ závisí od konkrétnych potrieb riadenia konkrétneho ochorenia. V niektorých aplikáciách manažérstva ochorení je potrebné, aby funkcia poplachu spustila poplach na upozornenie lekára alebo pacienta, aby bolo možné reagovať na kritický zdravotný stav. Prípustné oneskorenie pri týchto druhoch poplachov závisí od konkrétnych potrieb reagovania (napríklad ohrozenie života oproti vplyvu na pohodlie). Je tiež dôležité, aby sa mohli prístroje na manažérstvo ochorení konfigurovať (napríklad nastavenie periódy odosielania správ) a na overovanie správnej funkcie systému (skontrolovanie správnej funkcie senzorov, rovnako ako overovanie pripojenia).

4.2.2 Nezávislé starnutie

Aplikácia M2M na elektronické zdravotníctvo môže umožniť starším ľuďom nezávislý život a zotrvávanie vo svojich domovoch v prípadoch, kedy by za normálnych okolností potrebovali pomoc. Príklady zahŕňajú:

- diaľkový dohľad nad životne dôležitými funkciami pacienta (pulz, teplota, hmotnosť, krvný tlak), aby sa minimalizoval počet požadovaných návštev v ordinácii lekára;
- uistenie sa, že pacienti užívajú svoje lieky podľa požadovaného harmonogramu;
- sledovanie úrovne aktivity seniorov (napríklad čas strávený v posteli počas dňa, množstvo denného pohybu v ich domovoch) ako spôsobu posudzovania ich celkového zdravotného stavu a určovania zmien, ktoré môžu vyžadovať pozornosť lekára alebo nejakej inej osoby.

Rovnako ako v prípade manažérstva ochorení, aplikácie M2M na podporu nezávisle starnúcich alebo starších ľudí budú vyžadovať sledovanie zdravotného stavu a údajov o správaní. Hlavný mechanizmus tu tiež predstavuje nepretržitý zber údajov a ich presmerovanie na server na pozadí, ktorý poskytuje rozhranie pre lekárov a opatrovateľov (rodina, blízki), aby sa v prípade potreby vyvolala ich pozornosť.

4.2.3 Zlepšovanie fyzickej spôsobilosti osôb a zdravia

Aplikácie M2M v elektronickom zdravotníctve sa môžu používať na zaznamenávanie ukazovateľov zdravia a fyzickej spôsobilosti, ako sú frekvencia srdcových pulzov a frekvencia dýchania, spotreba energie, rýchlosť spaľovanie tukov atď. počas cvičenia. Môžu sa tiež používať na zaznamenávanie frekvencie a dĺžky cvičenia, intenzity cvičenia, dĺžky behu atď. Ak sa informácia odošle na server na pozadí, môže ju využívať lekár používateľa pri určovaní jeho zdravotného profilu a osobný tréner používateľa na poskytovanie spätnej väzby používateľovi o pokroku v jeho cvičebnom programe. To umožňuje prispôsobovať programy cvičenia alebo fyzioterapiu presnejšie a rýchlejšie podľa potrieb pacienta/používateľa.

Na rozdiel od aplikácií M2M na podporu manažérstva ochorenia a nezávislého starnutia podpora zlepšovania fyzickej spôsobilosti osôb a zdravia nebude s najväčšou pravdepodobnosťou vyžadovať časté zaznamenávanie alebo odosielanie dát a je tolerantnejšia k oneskoreniam pri odosielaní, pretože čas dostupnosti údajov nie je kritický.

5 Prípady používania aplikácií M2Mv elektronickom zdravotníctve

5.1 Diaľkový dohľad nad pacientom (RPM)

5.1.1 Všeobecný opis

Na najvyššej úrovni sa generický podrobný prípad používania diaľkového monitorovania zameriava na komunikáciu nameraných hodnôt vzdialených senzorov pacientov s podpornými systémami ošetrujúcich lekárov, EHR alebo osobným zdravotným záznamom (PHR) riadeným pacientom. V rámci komunikácie stroj-stroj sa prípad používania zameriava na prenos správ medzi vzdialenými monitorovacími zariadeniami a vrstvou poskytovateľa prvkov služby M2M. Architektonicky, prvky alebo rozhrania nad vrstvou poskytovateľa prvkov služby, ako podpora elektronických systémov používaných u lekárov na klinike alebo sprostredkovateľov, sú mimo rozsahu tohto dokumentu a sú zahrnuté len preto, aby poskytli systémové začlenenie. K obsiahnutej hlavnej problematike patrí obojsmerný prenos správ, dostupnosť siete v kritických momentoch, bezpečnosť informácií o sieti, bezpečné adresovanie zariadenia a označovanie správ.

5.1.2 Zainteresované subjekty

Pacient: „Pacient" môže byť každý jednotlivec alebo zástupca, ktorý by mohol používať vzdialené monitorovacie zariadenie na zhromažďovanie výsledkov meraní, dát alebo udalostí. Monitorovanie pacienta sa môže vykonávať v rôznych prostrediach, klinických ako sú nemocnice, alebo mimo klinických, napríklad v domácnosti, v práci, v škole, počas cestovania alebo v zariadeniach s asistenčnou službou.

Vzdialené monitorovacie zariadenie (RMD): Elektronické zariadenie M2M so senzorom, používateľské rozhranie alebo akčný člen a rozhranie do siete M2M. Zariadenie zhromažďuje informácie o pacientovi a komunikuje s príslušným poskytovateľom prvkov služby M2M a/alebo aplikáciou M2M pomocou siete M2M. RMD môže tiež komunikovať s týmito entitami pomocou sieťového priechodu M2M. Zariadenie môže prijímať a/alebo vykonávať príkazy od poskytovateľa prvkov služby M2M a/alebo aplikácie M2M alebo poskytovať informácie pacientovi. V týchto zariadeniach sa predpokladá nízka spotreba a jednoduché protokoly.

Poskytovateľ prvkov služby M2M: Entita siete, ktorá poskytuje komunikačné služby M2M entitám s aplikáciami M2M. Tieto aplikácie môžu podporovať konkrétne funkčné spôsobilosti, ktoré pomáhajú pri výmene príslušných zdravotných informácií. Navyše, poskytovateľ prvkov služby M2M komunikuje so vzdialeným monitorovacím zariadením, aby zozbieral dáta alebo vyslal príkazy.

Entita s aplikáciou M2M: Termín vytvorený na to, aby zainteresované subjekty nad rámec rozsahu M2M združil do celku a pracoval s nimi ako jedným systémovým prvkom. Aplikácie na vysokej úrovni, ako samostatná alebo geografická výmena zdravotných informácií, centrá na analýzu dát, siete poskytujúce integrovanú starostlivosť, organizácie poskytovateľov, banky zdravotných záznamov alebo verejné zdravotné siete, a/alebo špecializované siete sú všetko príklady entít s aplikáciami M2M. Termín entita s aplikáciou M2M tiež zahŕňa nasledujúce typické zainteresované subjekty RPM, ako sú:

Koordinátor starostlivosti: Koordinátor starostlivosti zahŕňa jednotlivcov alebo aplikácie v rámci dohľadu kliniky, kde sa sledujú informácie získané z prístroja/prístrojov pacienta. Koordinátor starostlivosti môže zasiahnuť, ak merania alebo výstrahy ukazujú, že došlo k zmene v zdravotnom stave pacienta, alebo ak sa výsledky meraní nachádzajú mimo stanoveného rozsahu. Koordinátor starostlivosti môže tiež informovať pacientovho lekára, ak meranie označuje potenciálny zdravotný problém.

Elektronický zdravotný záznam: Lekársky záznam, ktorý spravuje systém zdravotnej starostlivosti v digitálnej forme pre jednotlivca (EHR), alebo lekársky záznam spravovaný jednotlivcom alebo iný záznam (PHR).

Klinika: Ošetrujúci personál na klinike sú praktickí lekári, zdravotné sestry, sestry-lekárky, asistenti praktického lekára, psychológovia a ďalší pracovníci na klinike, ktorí klinicky vyhodnocujú diaľkové monitorovanie, v prípade potreby stanovujú vhodné klinické zásahy, aby mohli riadiť starostlivosť o pacientov.

5.1.3 Scenár

Inicializácia

Vzdialené monitorovacie zariadenie je pripravené na použitie a komunikáciu činnosťou pacienta alebo lekára na klinike. To môže vyžadovať fyzické pripojenie alebo umiestnenie zariadenia, registráciu zariadenia, nastavenie komunikačných kanálov s entitami aplikácií M2M, nastavenie komunikačných spôsobilostí zariadenia a poskytovanie bezpečnej komunikácie. V životne kritických aplikáciách sa môže pri inicializácii vyžadovať bezpečné overovanie totožnosti a overenie stavu zariadenia RMD poskytovateľom prvkov služby M2M a/alebo entitou aplikácie M2M.

Telemetria pacienta

Vzdialené monitorovacie zariadenie zhromažďuje merania od pacienta, údaje alebo udalosti. Údaje sa môžu prenášať vždy, keď zariadenie zhromaždí dáta, akumulované merania sa môžu prenášať pravidelne (napríklad každú hodinu, denne) alebo sa údaje môžu dodávať na požiadanie, alebo na základe určitých udalostí.

Ďalej možno požadovať, aby sa pri ohrození života alebo pri iných kritických meraniach alebo udalostiach nariadil a určil kritický čas ich odoslania. Pri týchto meraniach je potrebné často overovať stav zariadenia RMD sieťou prvku služby so spôsobilosťou M2M alebo entitou aplikácií M2M.

Dátové pakety sa posielajú sieťovej aplikácii M2M a smerujú do entity s aplikáciou M2M, a môže ich spravovať lekár, koordinátor starostlivosti alebo EHR.

Telemetrické dáta alebo existencia lekárskej telemetrie predstavujú informácie o pacientovi a samy osebe môžu vyžadovať ochranu súkromia.

V niektorých aplikáciách viacnásobné RMD posielajú telemetrické údaje o pacientovi, ktoré sa zbierajú, usporiadajú alebo inak ďalej spracúvajú sieťovým priechodom M2M, a len takto zozbierané, usporiadané alebo inak spracované údaje sa môžu poslať poskytovateľovi prvkov služby M2M alebo entitám s aplikáciami M2M.

Vzdialená konfigurácia

Vzdialené monitorovacie zariadenie sa môže nakonfigurovať pomocou siete M2M entitami aplikácie M2M. Spôsobilosť konfigurácie môže zahŕňať jednoduché zmeny parametrov, ako je rýchlosť odovzdávania správ, úrovne udalostí alebo spúšťanie výstražného signálu a úrovne dávkovania na sťahovanie a bezpečné reštartovanie nového operačného softvéru.

Vyžaduje sa bezpečné, objednané a potvrdené zasielanie správ.

Tiež sa požaduje potvrdenie správy od RMD o vzdialenej konfigurácii a o dosiahnutí požadovaného stavu konfigurácie.

V niektorých aplikáciách poskytovateľ prvkov služby M2M diaľkovo konfiguruje viaceré RMD, s rovnakými alebo špecifickými nastaveniami. Sieťové priechody M2M môžu distribuovať

niektoré alebo všetky tieto konfiguračné správy viacerým zariadeniam RMD, ktoré sú k nim pripojené.

Konfigurácia prístroja alebo typ prístroja sú informáciou o pacientovi a osobitne môže vyžadovať ochranu súkromia.

Diaľkové ovládanie

RMD môže slúžiť pacientovi alebo s ním komunikovať. Riadenie môže zahŕňať časovo kritické alebo objednané prvky, aby sa zabezpečilo jednorazové dávkovanie alebo sa zaistili elektrické impulzy v jednoduchých textových správach, ktoré vyžadujú činnosť pacienta alebo odpoveď.

Pre väčšinu aplikácií majú byť správy diaľkového ovládania bezpečné. Ďalej sa môže požadovať overovanie totožnosti alebo stavu integrity RMD, ktorý prijíma správu diaľkového ovládania.

V niektorých aplikáciách môžu viaceré RMD prijať rovnaké alebo jednotlivo zamerané správy diaľkového ovládania od poskytovateľa prvkov služieb M2M. Sieťové priechody M2M môžu distribuovať také viacnásobné správy diaľkového ovládania k zariadeniam RMD, ktoré sú k nim pripojené.

5.1.4 Výmena informácií

Registrácia

Prístroj komunikuje s poskytovateľom prvkov služby M2M, aby sa zabezpečila inicializácia prístroja v systéme M2M. Registrácia zahŕňa schopnosť udržiavať informácie opisujúce vzdialené monitorovacie zariadenie, monitorovaného pacienta (ak sa súkromie nepovažuje za problém, je v súlade s politikami a pacient to vopred odsúhlasil) a aplikáciu M2M, ktorá bude skúmať sledované dáta. Napríklad to môže zahŕňať registráciu prístroja u výrobcu alebo sprostredkovateľa dát a vykonávanie ďalších funkcií na jednoznačnú identifikáciu prístroja. Registrácia môže tiež zahŕňať registráciu dát, ktoré sa môžu použiť na overenie stavu zariadenia RMD poskytovateľom prvkov služby M2M.

Vyhľadávanie dát

Schopnosť lokalizovať a vyhľadať požadované dáta, ktoré sú predmetom prístupových práv a miestnych politík. Dáta diaľkového monitorovania sa prijímajú pomocou poskytovateľa prvkov služby M2M a sú spájané s príslušnými príjemcami dát.

Doručovanie dát

Schopnosť bezpečne doručiť dáta do určeného zariadenia alebo poskytovateľovi prvkov služby M2M a potvrdiť doručenie, vrátane možnosti v prípade potreby smerovať dáta na základe obsahu správy. Napríklad kritické životné udalosti sa musia smerovať do veľmi spoľahlivých kanálov so zaručeným časom dodania.

5.1.5 Potenciálne nové požiadavky

5.1.5.1 Inicializácia a registrácia zariadenia

Článok opisuje kroky, potrebné na inicializáciu a registráciu RMD a na nadviazanie komunikácie, ktoré môžu vyžadovať opatrenie zo strany pacienta i lekára.

Prednostne treba vykonať takéto kroky:

1. RMD môže vyžadovať fyzické pripojenie zariadenia k notebooku alebo inému zariadeniu, ktoré umožní počiatočný prenos informácií.

2. RMD by malo po zapnutí spustiť počiatočnú sekvenciu, ktorá môže vykonať základné diagnostické kontroly, aby sa overilo, či zariadenie funguje správne.

3. Niektoré životne dôležité aplikácie môžu vyžadovať, aby zariadenie vykonávalo bezpečný postup štartovania, ktorý zahŕňa kontrolu integrity. Porucha zdravotného zariadenia/aplikácie pri overovaní integrity zariadenia má zablokovať registráciu a voliteľne upozorniť používateľa na poruchu zariadenia.

4. Po úspešnej inicializácii RMD začne vykonávať registračné postupy.

5. Zdravotné zariadenia/aplikácie pacienta a poskytovateľa sa nezávisle overujú a registrujú vo vrstve prvkov služby a vyhlásia/potvrdia svoje požiadavky na triedu služby (a triedu zariadenia).

6. Ak je žiadosť platná, systémy sú autentizované a autorizované.

7. Preklad názvu/adresy sa uskutoční kvôli smerovaniu.

8. Stanovia sa komunikačné spôsobilosti a konfigurácia.

Mapovanie funkcií uvedených krokov je nasledujúce:

1. Zariadenie RMD môže vyžadovať fyzické pripojenie (napríklad cez USB) na počiatočnú konfiguráciu zariadenia.

2. Overenie RMD pre kritické životné funkcie by malo vykonávať overenie založené na dôveryhodnom prostredí realizácie.

3. Neúspešná inicializácia RMD by mala spustiť signalizáciu porúch na zariadení.

4. Aplikácia M2M (v doménach siete a zariadenia) sa registruje v entite so spôsobilosťou služby, aby sa určila činnosť.

5. Sieťový priechod M2M (ak sa použije) prenáša (smeruje) žiadosť o registráciu do siete (zriadi prístup k potrebným prvkom v sieti).

6. Príslušná entita so spôsobilosťou služby vykonáva registráciu, autentizáciu, autorizáciu aplikácií M2M a zabezpečuje konektivitu s inými prvkami.

7. Entita so spôsobilosťou služby sleduje a zaznamenáva začiatočnú registráciu a deaktiváciu zariadenia alebo sieťového priechodu M2M. Entita môže tiež vykonávať preklad názvu.

8. Entita so spôsobilosťou služby poskytuje mapovanie adries a mien, a monitoruje stav zariadenia.

9. Entita s vhodnou spôsobilosťou služby vyberá sieťové adresy z aplikácie M2M. Zabezpečuje aj výber siete (založený na triede služieb a ďalších faktoroch) pre zariadenia, ktoré podporujú viac sietí alebo komunikačných služieb.

10. Registrácia RMD by mala podporovať bezpečné uchovávanie citlivých dát pacientov.

5.1.5.2 Komunikácia zariadenia

5.1.5.2.1 Diaľkové riadenie a konfigurácia

Článok opisuje diaľkovú komunikáciu medzi používateľom (pacient alebo poskytovateľ) a zariadením alebo aplikáciou M2M. Príklady tejto komunikácie zahŕňajú diaľkovú konfiguráciu a diaľkové ovládanie zariadenia, poskytovateľov hľadajúcich údaje vo vzdialenom

monitorovacom zariadení alebo pacienta aktualizujúceho EMR (alebo zdravotnú databázu) nejakými relevantnými informáciami.

Pri tomto type komunikácie sa vykonávajú nasledujúce kroky:

1. Poskytovateľ alebo pacient sa prihlási do systému bezpečného zasielania správ pomocou svojej identity používateľa a hesla (a akýchkoľvek iných bezpečnostných prihlasovacích údajov).
2. Používateľ (pacient alebo poskytovateľ) vyberie činnosť a zariadenie, s ktorým by radi komunikovali (v niektorých prípadoch zariadenia v tom čase nemusí byť online).
3. Používateľ zadá nové informácie alebo dopyt na zariadenie.
4. Aplikácia kontaktuje zariadenie s požiadavkou. To sa uskutoční v reálnom čase alebo neskôr, keď sa zariadenie pripojí.
5. Odosielateľ informácie dostane správu o stave žiadosti a poskytne sa mu informácia (ak je k dispozícii).

Mapovanie funkcií uvedených krokov je takéto:

1. Životne dôležité M2M RMD by malo zabezpečovať bezpečný prenos a príjem pri výmene správ pomocou bezpečného protokolu.
2. AAA entita bezpečného zasielania správ v sieti overuje a autorizuje používateľa.
3. Sieť analyzuje správu na zistenie identity zariadenia.
4. Entita s vhodnou spôsobilosťou služby potvrdí, že zariadenie je registrované a vyhľadá mapovanie mena na adresu siete. Zabezpečí aj výber siete (založený na triede služby a ďalších faktoroch) pre zariadenia, ktoré podporujú viac sietí alebo komunikačné služby.
5. Entita s vhodnou spôsobilosťou služby skontroluje aktuálny stav zariadenia (dosiahnuteľné alebo nie) a poslednú známu trasu.
6. Vhodná spôsobilosť služby môže poskytnúť aj spoplatňovanie záznamov za použitie prvkov.
7. Entita s vhodnou spôsobilosťou služby monitoruje a zabezpečuje konfiguráciu, prevádzku a funkcie spravovania porúch (sleduje výmenu správ z pohľadu chybovosti, porúch atď.).
8. Entita s vhodnou spôsobilosťou služby bude prenášať správy medzi aplikáciou bezpečného zasielania správ a zariadením M2M cez sieťový priechod M2M v prípade potreby. Spracúva retransmisie, hlási chyby, skrýva nepotrebné informácie a monitoruje stav doručenia.
9. Entita s vhodnou spôsobilosťou služby uchováva kópie správ a stavu doručenia, chybové hlásenia atď.
10. Sieťový priechod M2M (ak sa použije) prenáša (alebo smeruje) správu do siete.
11. Zariadenie M2M prijme správu.
12. Entita s vhodnou spôsobilosťou služby pošle odosielateľovi aktualizovaný stav správy a požadované informácie (ak sa požadujú).
13. RMD by malo poskytnúť spracovanie a doručenie časovo naliehavých správ.

14. M2M RMD by malo zabezpečiť bezpečné uchovávanie osobných pacientových informácií.

5.1.5.2.2 Telemetria pacienta (vyhľadávanie a distribúcia dát)

Článok opisuje komunikáciu od RMD (alebo aplikácie v RMD) k poskytovateľovi (alebo službe M2M).

Nasledujúce kroky sa vykonávajú pri tomto type komunikácie:

1. Podľa vopred určeného plánu alebo na základe nejakej udalosti (pravidelnej alebo v režime požiadania informácie o správe) sa zariadenie „prebudí" a zaregistruje sa v sieti, ak už nie je pripojené.

2. Ak sieť nie je k dispozícii, potom sa správa uloží a vykonajú sa pokusy o pripojenie na sieť vo vopred definovaných intervaloch.

3. Po pripojení sa správa pripraví a odošle.

4. Správa sa doručí (ak doručenie zlyhá, skúšajú sa samočinné retransmisie).

5. Stav doručenia správy sa oznámi späť do odosielajúceho zariadenia M2M (alebo aplikácie).

6. Možno požadovať, aby sa pri ohrození života alebo pri iných kritických meraniach alebo udalostiach nariadil a zaručil kritický čas ich odoslania.

7. Možno požadovať, aby sa pri ohrození života často overovalo RMD sieťou služby so spôsobilosťou M2M alebo entitou aplikácií M2M.

8. Možno požadovať, aby sa pri ohrození života podporovala komunikácia so záchrannou službou alebo sa zabezpečilo smerovanie špecializovaných správ v rámci systému M2M (t. j. oznámenie o dôležitých informáciách o pacientovi zodpovedajúcim pracovníkom záchrannej služby).

Mapovanie funkcií uvedených krokov je nasledujúce:

1. Nevyhnutný predpoklad: zariadenie M2M sa aktivuje a zaregistruje do siete (podrobne v predchádzajúcom článku).

2. Zariadenie M2M pripraví a vyšle správu.

3. Sieťový priechod M2M (ak sa použije) prenáša (alebo smeruje) správu do siete.

4. Entita s vhodnou spôsobilosťou služby vykonáva smerovanie na spôsobilosti služby podľa potreby a môže tiež zabezpečiť spoplatňovanie záznamov na využitie spôsobilosti.

5. Entita s vhodnou spôsobilosťou služby vyberie názov a informácie o pripojení z aplikácie M2M a funkcie manažérstva. Tiež monitoruje a zabezpečuje konfiguráciu, prevádzku a funkcie chybového manažérstva (sleduje výmenu správ z pohľadu chybovosti, porúch atď.).

6. Entita s vhodnou spôsobilosťou služby bude prenášať správy medzi zariadením M2M, sieťovým priechodom M2M a aplikáciou M2M (v sieti). Spracuje retransmisie, hlási chyby, skrýva zbytočné informácie a monitoruje stav doručenia.

7. Entita s vhodnou spôsobilosťou služby uchováva kópie správ a stav doručenia, chybové hlásenia atď.

8. Aplikácia M2M (zariadenie alebo sieťová doména) prijme správy.

V životne dôležitom RMD platia tieto funkcionality:

1. M2M RMD má podporovať spoľahlivé a zaručené doručenie správy.
2. M2M RMD má podporovať presnú a bezpečnú časovú synchronizáciu.
3. M2M RMD má podporovať výber a použitie vhodných komunikačných kanálov, aby sa zaistil spoľahlivý prenos v kritickej životnej udalosti (udalostiach).
4. M2M RMD má zabezpečiť doručovanie správ podľa poradia s ohľadom na prednostné spracovanie prvkov služby.
5. M2M RMD má podporovať prioritnú komunikáciu so záchrannými službami.

5.1.5.3 Odvodené potenciálne nové požiadavky

Nasledujúce potenciálne nové požiadavky na systém M2M:

1. Overenie integrity v dôveryhodnom prostredí realizácie.
2. Signalizácia porúch pri zistení zlyhaní inicializácie.
3. Podpora bezpečného uchovávania citlivých dát.
4. Podpora bezpečnej komunikácie pomocou bezpečného protokolu.
5. Podpora spracovania správy a jej doručenia v požadovanom čase.
6. Podpora bezpečnej časovej synchronizácie.
7. Podpora doručenia správy podľa poradia na základe prednostného spracovania služby.
8. Podpora prednostnej komunikácie v prípade časovo citlivých zdravotných služieb.

Podrobné mapovanie prednostných tokov a funkcií do základných komunikačných entít opisujú predchádzajúce články, aby sa doplnilo zdôvodnenie, prečo sa tieto položky označujú ako potenciálne nové požiadavky.

5.2 Bezpečné zasielanie správ pacient – poskytovateľ

5.2.1 Všeobecný opis

Termín „bezpečné zasielanie správ pacient-poskytovateľ" zahŕňa bezpečné správy medzi pacientmi a poskytovateľmi, ktoré zahŕňajú aspoň jedno zariadenie alebo aplikáciu M2M. Použitý termín „poskytovateľ" zahŕňa lekárov a aj zdravotnícky pomocný personál. Tento prípad používania obsahuje nasledujúce scenáre zasielania správ:

1. Zariadenie M2M (alebo systém/aplikácia) k zariadeniu M2M (alebo systému/aplikácii).
2. Zariadenie M2M (alebo systém/aplikácia) k používateľovi (pacientovi alebo poskytovateľovi).
3. Používateľ (pacient alebo poskytovateľ) k zariadeniu M2M (alebo systému/aplikácii).

Prípad používania nezahŕňa zasielanie správ medzi pacientom a poskytovateľom, ktoré sú typu používateľ-používateľ. To môže obsahovať napríklad otázky a odpovede na príznaky a liečbu, poskytovanie ručne zhromaždených informácií alebo otázok o existujúcom vlastnom sledovaní alebo starostlivosti o skupiny chronicky chorých atď.

Táto forma komunikácie má schopnosť zvýšiť všeobecnú starostlivosť ako aj riadenie podmienok starostlivosti o chronicky chorých. Komunikácia môže prebiehať mnohými

spôsobmi, ale najčastejšie to bude prostredníctvom bezpečného zasielania správ. Osobné zdravotné informácie obsiahnuté v týchto správach sa budú musieť poskytovať pomocou bezpečného vysielania a prijímania. Tieto informácie, keď sa ukladajú a spracúvajú v zariadeniach a systémoch M2M, majú mať tiež chránenú integritu alebo zostať dôverné. Uzly zariadení a systémov M2M (napríklad sieťové priechody, servery atď.), ktoré spracúvajú tieto informácie majú byť bezpečné a dôveryhodné.

Na podporu tohto typu aplikácie elektronického zdravotníctva sa prednostne musia podporovať nasledujúce požiadavky (alebo scenáre):

- podpora komunikácie iniciovanej pacientom (pomocou pacientovho zariadenia M2M);
- podpora komunikácie iniciovanej poskytovateľom (pomocou servera alebo zariadenia aplikácie M2M poskytovateľa);
- podpora komunikácie založenej na politike, udalosti alebo rozvrhu;
- podpora smerovania dát na základe obsahu;
- vzájomná spolupráca (dátový formát atď.).

5.2.2 Zainteresované subjekty

Prípad používania zahŕňa nasledujúce zainteresované subjekty:

- pacient – ten, kto dostáva zdravotné služby;
- opatrovatelia pacienta – opatrovatelia, obhajcovia pacientov, zástupcovia, rodinní príslušníci a ďalšie osoby, ktoré môžu konať v prospech alebo na podporu pacienta, ktorý prijíma alebo potenciálne bude prijímať zdravotné služby;
- poskytovateľ:
  - lekár – poskytovatelia zdravotnej starostlivosti s povinnosťou starostlivosti o pacienta, vrátane praktických lekárov, zdravotných sestier s pokročilou praxou, asistentov praktických lekárov, zdravotných sestier, psychológov, farmaceutov a ostatných oprávnených a poverených pracovníkov, ktorí sa zaoberajú liečením pacientov;
  - podporný personál lekára – jednotlivci, ktorí podporujú pracovný postup lekárov; napríklad administratívni pracovníci, ktorí spočiatku prijímajú a vyhodnocujú správy od pacientov, a podnikajú príslušné kroky;
- entity zdravotnej starostlivosti – organizácie, ktoré sa zaoberajú poskytovaním zdravotnej starostlivosti alebo ju podporujú; tieto organizácie môžu zahŕňať nemocnice, ambulantné kliniky, zariadenia dlhodobej starostlivosti, komunitné zdravotné organizácie, lekárne atď.;
- zdravotnícke monitorovacie/telemetrické zariadenie – zariadenie na monitorovanie a poskytovanie údajov súvisiacich so zdravím od pacienta k poskytovateľovi alebo k inej zdravotníckej entite;
- databáza zdravie/EMR/PHR/ – elektronická aplikácia, softvér alebo prostriedok, ktorý monitoruje starostlivosť o pacienta a pomáha ju spravovať;
- dodávatelia databázy zdravie/EMR/PHR/ – organizácie, ktoré poskytujú konkrétne riešenia EHR a PHR poskytovateľom a pacientom, ako sú softvérové aplikácie a softvérové služby.

Dodávatelia zdravotníckych pomôcok – organizácie, ktoré poskytujú zdravotnícke pomôcky alebo prípravky na pomoc pri odstraňovaní zdravotných ťažkostí a pri liečení chorôb. Tieto prístroje alebo pomôcky môžu podporovať monitorovanie fyziologických funkcií, bezpečné zasielanie správ a zasielanie obsahu.

5.2.3 Scenár

5.2.3.1 Kategórie a platformy bezpečného zasielania správ

5.2.3.1.1 Zariadenie M2M (alebo systém/aplikácia)-zariadenie M2M (alebo systém/aplikácia)

Kategória správ obsahuje správy, ktoré samostatne odosiela zariadenie dohliadajúce na zdravotný stav, systém lekárskeho záznamu, senzory atď., do iného zariadenia alebo aplikácie M2M. Kategória nezahŕňa žiadny zásah používateľa. Príklady obsahujú pravidelné správy o fyziologických údajoch posielané z prístrojov monitorujúcich pacienta k poskytovateľovmu EMR (alebo zdravotnej databázy). Môže tiež obsahovať systém EMR poskytovateľa (alebo podobnú aplikáciu), ktorý samostatne odosiela žiadosti o namerané hodnoty alebo informácií o konfigurácii na zariadenie monitorujúce zdravotný stav pacienta.

5.2.3.1.2 Zariadenie M2M (alebo systém/aplikácia)-používateľ (pacient alebo poskytovateľ)

Kategória správ obsahuje správy, ktoré odosiela zariadenie alebo aplikácia M2M, kde príjemcom je používateľ (pacient alebo poskytovateľ). Príklady zahŕňajú zariadenie dohliadajúce na zdravotný stav pacienta, ktoré upozorní poskytovateľa alebo centrum pohotovostnej zdravotnej starostlivosti o dôležitých životných funkciách, a rovnako systém poskytovateľa EMR, ktorý autonómne odosiela pacientovi pripomienky, pokiaľ ide o každoročné fyzické prehliadky, odborné vyšetrenia, očkovanie alebo iné liečebné postupy.

5.2.3.1.3 Používateľ (pacient alebo poskytovateľ)-zariadenie M2M (alebo systém/aplikácia)

Kategória správ obsahuje správy, ktoré odosiela pacient alebo poskytovateľ zariadeniu alebo aplikácii M2M. Príklady zahŕňajú požiadanie poskytovateľa o vzdialené monitorovacie zariadenie na odčítanie údajov, konfiguráciu takéhoto zariadenia alebo aktualizáciu pacientovho EMR (alebo zdravotnej databázy) nejakými relevantnými informáciami.

5.2.3.1.4 Platformy zasielania správ

Dve z troch uvedených kategórií zasielania správ môžu zahŕňať rôzne platformy, kde jedna strana predstavuje zariadenie alebo aplikáciu M2M a na druhej strane je všeobecnejšia počítačová platforma, ktorá podporuje bezpečný systém zasielania správ alebo aplikácie, pomocou ktorých dokáže pacient alebo poskytovateľ správy odoslať alebo prijať. Napríklad pacient môže mať zariadenie na sledovanie zdravotného stavu, ktoré oznamuje fyziologické dáta a má oddelenú bezpečnú webovú aplikáciu na zasielanie správ alebo beží v notebooku pri ručnom inicializovaní zasielania správ. Prípadne môže spoločná platforma podporovať obidve funkcie. Samozrejme, v každom prípade sa musia použiť správne postupy, aby sa zabezpečilo bezpečné spracovanie, dôvernosť a integrita dát.

5.2.4 Výmena informácií

5.2.4.1 Počiatočné nastavenie bezpečného zasielania správ

5.2.4.1.1 Komunikácia iniciovaná používateľom

Pred využitím funkcie bezpečného zasielania správ budú pacienti a poskytovatelia podnikať kroky na nastavenie svojho prístupu k systému. To zahŕňa vytvorenie nevyhnutných

bezpečnostných informácií (overenie identifikácie používateľa atď.), rovnako ako inštaláciu všetkých potrebných bezpečnostných aplikácií (alebo protokolov), ktoré musia byť v prevádzke v systéme koncového bodu (ako je notebook, inteligentný telefón atď.).

Činnosť pri zasielaní správ môže využívať existujúce bezpečnostné mechanizmy (napríklad prístup a bezpečné protokoly aplikácií) v sieti a môžu vyžadovať ďalšie špecifické bezpečné spôsobilosti M2M, ako je overovanie platformy. Okrem toho môže byť potrebné, aby systém zvládol nízky výkon a komplexné bezpečnostné požiadavky na určité triedy zariadení, ako sú senzory na telo atď.

Bezpečný systém zasielania správ môže prebiehať niekoľkými spôsobmi:

- spojením bod-bod
  - spôsob zabezpečuje priamu interakciu priamo medzi dvoma systémami bez potreby medziľahlých smerovacích funkcií; tieto koncové body môžu byť súčasťou rôznych aplikácií na zasielanie správ alebo iných platforiem so spoločnou aplikáciou;
- pomocou webu
  - bezpečný prenos správ sa spolieha na internet a podporujú ho spoločné alebo oddelené (alebo odlišné) aplikácie pacienta a poskytovateľa.

5.2.4.1.2 Komunikácia iniciovaná zariadením

Pred inštaláciou zdravotného zariadenia/systému a aplikácie poskytovateľ systému získa súhlas od poskytovateľa prvkov služby na súbor funkcionalít, ktoré aplikácia vyžaduje alebo má na ne prístup.

To bude zahŕňať informácie, ako požiadavky na triedu zariadenia a služby, podpora prístupovej technológie, oprávnených používatelia atď.

V čase inštalácie zariadenia alebo systému je potrebná určitá konfigurácia, aby sa zabezpečilo príslušné pripojenie, prístup používateľa atď. V mnohých prípadoch, vo väčšine, ak nie vo všetkých, konfigurácia sa môže a mala by sa automatizovať (automatické konfigurovanie), aby používateľ nemusel mať podrobné vedomosti o použitej technológii. Môže existovať niekoľko málo požiadaviek na potrebnú konfiguráciu, ktoré sa dajú ľahko zvládnuť pomocou používateľského rozhrania, ktoré vyzve používateľa na zadanie potrebných informácií. Je pravdepodobné, že táto potrebná ručná konfigurácia sa viac zameria na prístup používateľa k zariadeniu (alebo aplikácii/systému) a súvisiace vlastnosti.

5.2.4.2 Komunikácia iniciovaná pacientom

5.2.4.2.1 Komunikácia iniciovaná používateľom

Pacienti môžu iniciovať komunikáciu s EMR poskytovateľa alebo aplikáciou zdravotnej databázy pomocou prostriedku na bezpečné zasielanie správ na rôzne účely. Príklady zahŕňajú poskytovanie ručne zhromaždených informácií o existujúcom vlastnom sledovaní alebo starostlivosti o skupiny chronicky chorých.

Pri odoslaní týchto správ sa pacient musí prihlásiť do systému bezpečného zasielania správ pomocou svojej identity používateľa a hesla (a akýchkoľvek ďalších bezpečnostných oprávnení) a napísať, a odoslať správu.

Ak EMR poskytovateľa alebo aplikácia zdravotnej databázy prijíma a spracováva správu od pacienta, môže upozorniť poskytovateľa na aktualizáciu a prípadne odovzdať informácie ďalším príslušným zainteresovaným subjektom. Pacient dostane informáciu, že správa bola prijatá a spracovaná prostredníctvom automatickej odpovede od EMR, alebo, ak je to

potrebné, bude ho poskytovateľ kontaktovať priamo pomocou bezpečnej správy alebo telefonickým hovorom.

5.2.4.2.2 Komunikácia iniciovaná zariadením

Zariadenia dohliadajúce na zdravotný stav pacienta môžu začať komunikáciu (samostatne) s poskytovateľom pomocou mechanizmu bezpečného zasielania správ s nasledujúcimi zámermi:

- pravidelné správy s fyziologickými údajmi (z rôznych zdravotníckych pomôcok) na základe vopred stanoveného rozvrhu;
- správy s fyziologickými údajmi založené na udalosti (alebo prahovej hodnoty) .

Zariadenie bude tiež využívať mechanizmus bezpečného zasielania správ na prenos týchto údajov. Architektúra funkcionality M2M bude preto musieť podporovať potrebné bezpečné funkcie.

Samostatná správa sa doručí do aplikácie/systému M2M poskytovateľa. Môže to byť systém v priestoroch poskytovateľa (alebo v nemocnici atď.) alebo v informačnom centre, ktoré zabezpečuje uchovávanie a zber dát pre poskytovateľa. Tieto údaje sa zaznamenajú do EMR pacienta a poskytovateľ sa upozorní o prijatí tejto správy. To sa môže vykonať akýmkoľvek systémom nezabezpečeného zasielania správ, pretože nebude obsahovať žiadne osobné údaje pacienta.

Ak správa predstavuje periodické oznamovanie údajov, nemusí poskytovateľ prijať okamžité opatrenie k tejto správe. Je pravdepodobné, že údaje sa budú skúmať v rámci nasledujúcej plánovanej návštevy pacienta.

Všeobecne platí, že udalosti zakladajúce sa na správach patria do dvoch kategórií. Do prvej kategórie patria tiesňové udalosti, ktoré vyžadujú okamžitú pozornosť. Druhou kategóriou sú udalosti, ktoré nepotrebujú okamžitú pozornosť, ale prihlásia sa do EMR poskytovateľa alebo aplikácie zdravotnej databázy. Možné akcie pri každej z týchto správ zakladajúce sa na udalosti, sú nasledujúce:

- správy o tiesňovej udalosti – v tomto prípade zariadenie M2M sa nastaví tak, aby sa kontaktovali záchranné služby a vyslala sa aj naliehavá bezpečná správa. Informácie poskytnuté záchranným službám budú zahŕňať povahu prípadu núdze, informácie o pacientovi a o umiestnení pacienta;
- správy o tiesňovej udalosti – v tomto prípade zariadenie M2M oznámi údaje o udalosti poskytovateľovi EMR alebo aplikácii zdravotnej databázy a poskytovateľ sa upozorní, že túto udalosť systém zaznamenal; poskytovateľ túto správu posúdi pri ďalšej naplánovanej návšteve ordinácie alebo kontrole, alebo skôr v závislosti od nastavenia kritérií udalostí v systéme.

Obyčajne, zariadenie možno nakonfigurovať (možno v predvolenom nastavení) tak, aby si vyžiadalo potvrdenie o doručení správy príjemcovi alebo o jej prečítaní príjemcom. Neprítomnosť takéhoto potvrdenia, najmä v prípade správy založenej na udalosti (ktorá môže byť svojou podstatou kritická) by mala predstavovať podnet pre zariadenie, aby vykonalo alternatívnu činnosť. Táto činnosť môže zahŕňať pokus o komunikáciu alternatívnou technológiou prístupu, odovzdanie správy do iného strediska prvej pomoci alebo poskytovateľovi, presmerovanie na iných opatrovateľov (rodinu atď.), rovnako ako upozornenie priamo pacienta.

5.2.4.3 Komunikácia iniciovaná poskytovateľom

5.2.4.3.1 Komunikácia iniciovaná používateľom

Poskytovatelia môžu nadviazať komunikáciu so zariadením dohliadajúcim na zdravotný stav pacienta z viacerých dôvodov. Príklady zahŕňajú dopyt sprostredkovateľa na zariadenie z dôvodu odčítania údajov alebo konfigurácie takéhoto zariadenia.

Pri odoslaní týchto správ sa poskytovateľ musí prihlásiť do systému bezpečného zasielania správ pomocou svojej identity používateľa a hesla (a akýchkoľvek ďalších bezpečnostných oprávnení) a napísať, ako aj odoslať správu do zariadenia či systému pacienta.

5.2.4.3.2 Komunikácia iniciovaná zariadením

Poskytovatelia systému EMR (alebo podobnej aplikácie) môžu samostatne iniciovať komunikáciu s pacientom z viacerých dôvodov. Komunikácia sa môže nasmerovať na pacienta alebo na zariadenie dohliadajúce na zdravotný stav pacienta. Dôvody sú nasledujúce:

- pripomenúť pacientom ročné fyzické vyšetrenia, odborné vyšetrenia, očkovania atď.
- vydať nové kritériá na vykazovanie, vzhľadom na zariadenie dohliadajúce na zdravotný stav pacienta, aby zmenilo rozvrh podávanie správ, úrovne medzných udalostí atď. (môže byť potrebná ručná inicializácia);
- zaviesť novú požiadavku/spôsobilosť merania na zariadenie dohliadajúce na zdravotný stav (môže byť potrebná ručná inicializácia).

Tradičná (nezabezpečená) elektronická alebo textová správa sa tiež môže použiť na upozornenie pacienta, že mu bola odoslaná zabezpečená správa a mal by si skontrolovať systém bezpečných správ, aby ju mohol prijať. Okrem toho môže byť tiež upozornený na vykonané aktualizácie v programe zariadenia na sledovanie zdravotného stavu (alebo aplikácií). Použitie tradičného elektronického alebo textového zasielania správ zvýši istotu, že pacienti správy dostanú, aj keď nemôžu mať prístup alebo nie sú prihlásení do systému bezpečných správ.

5.2.4.4 Iná výmena informácií

5.2.4.4.1 Smerovanie dát na základe obsahu

V uvedených scenároch sa systém môže nakonfigurovať tak, aby umožnil smerovanie dát v závislosti od obsahu. Niekoľko príkladov zahŕňa:

- správa založená na udalosti (alebo prahu) zo zariadenia dohliadajúceho na zdravotný stav, okrem správy vyslanej do pracovne poskytovateľa, môže sa tiež smerovať na pohotovosť alebo stredisko kritickej starostlivosti, ak správa označuje urgentný stav ohrozujúci život;
- ak poskytovateľ objednáva nové testy alebo nový recept, správa sa môže vyslať nielen pacientovi, ale aj do laboratória a lekárne, aby sa urýchlila služba;
- správy od poskytovateľa sa môžu tiež smerovať k povereným opatrovateľom alebo koordinátorom, členom rodiny atď. v závislosti od povahy správy.

S cieľom podporiť smerovanie založené na obsahu, tretie strany, ktorým je povolené získavať tieto informácie, musia byť vopred autorizované pacientom a systémom.

5.2.4.4.2 Vzájomná spolupráca (dátový formát atď.)

V závislosti od konkrétneho typu informácií, ktoré sa prenášajú medzi pacientom a poskytovateľom v bezpečných správach, sa údaje môžu poskytovať pomocou rôznych formátov. Pri správach v ručne zabezpečovanej komunikácii sa môže používať štruktúrovaná šablóna (rozbaľovacie menu atď.), neštruktúrovaná šablóna (voľný text) alebo ich kombinácia. Systém zasielania správ má zaistiť logické oddelenie dát a týmto spôsobom zvýšiť tok informácií.

V správach v samostatne zabezpečovanej komunikácii majú byť zdravotné údaje ako napríklad namerané hodnoty zo zariadenia dohliadajúceho na zdravotný stav (krvný tlak, glukóza atď.), v súlade s normou, ktorá definuje formát a štruktúru týchto informácií. To zabezpečuje interoperabilitu medzi systémami a aplikáciami.

Vynakladá sa veľa úsilia na vytvorenie spoločnej normy na lekárske záznamy a údaje, ktoré sa môžu používať. Tieto snahy zahŕňajú HL7, Európsky inštitút zdravotných záznamov (EuroRec Institute) atď.

5.2.5 Potenciálne nové požiadavky

5.2.5.1 Aktualizácia bezpečných protokolov

Aktuálne zostavy bezpečného zasielania správ ako PGP a TLS nemusia predstavovať dostatočný rámec na spracovanie dôveryhodnej komunikácie. Existujú predpisy, ktoré sa týkajú uchovávania, prenosu alebo zničenia elektronických zdravotných informácií. Tieto predpisy sú v rámci rôznych jurisdikčných regiónov nekompatibilné. Z tohto dôvodu na spracovanie dôveryhodnej komunikácie môžu byť potrebné rozšírenia.

Aj niektoré zariadenia elektronického zdravotníctva alebo senzory nemusia podporovať potrebný hardvér alebo softvér, vzhľadom na ich veľkosť a obmedzenia spracovania. V takých prípadoch je potrebné, aby kapilárne siete a sieťové priechody podporovali nasledujúce požiadavky.

Na zabezpečenie výmeny informácií musí systém podporovať tieto konkrétne požiadavky:

- bezpečnosť a dôveryhodnosť zariadenia;
- dôvernosť a ochrana súkromia pri výmene informácií;
- integrita vymieňaných informácií;
- ochrana (integrity a dôvernosti) dát pri uchovávaní v zariadeniach;
- ochrana dát, ak sú spracovávané v zariadeniach.

5.2.5.2 Prenositeľnosť pripojenia

Využitie zariadení M2M na monitorovanie informácií o zdraví sa neobmedzuje iba na bydlisko pacienta. Zariadenie M2M a podporný systém (a aplikácia) poskytne možnosť pripojenia na sieťové priechody M2M (alebo rovnocenné komponenty) na iných miestach, a tým sa vytvorí pripojenie na sieť a k príjemcom dátových hlásení alebo správ. Okrem možnosti pripojiť sa na alternatívne sieťové priechody M2M sa zariadenie ubezpečí, že sieťový priechod predstavuje bezpečný a dôveryhodný systém, ktorý bude podporovať bezpečný prenos informácií. Požiadavka môže alebo nemusí obsahovať požiadavku na nepretržité pripojenie. To by znamenalo, že zariadenie/pripojenie môže podporovať odovzdávanie medzi rôznymi sieťovými priechodmi, základňovými stanicami alebo prístupovými technológiami.

5.2.5.3 Sledovanie umiestnenia

Spolu s požiadavkou na prenositeľnosť, uvedenou v predchádzajúcom článku, zariadenie M2M a podporný systém (a aplikácia) budú schopné sledovať a hlásiť pacientovo umiestnenie. Informácia môže byť rozhodujúca v núdzových situáciách pri poskytovaní informácií o umiestnení pre EMT alebo ambulantné služby, o blízkosti okolitých nemocníc atď.

5.2.5.4 Zdôvodnenie

Podrobné prednostné kroky a funkčné mapovanie do základných komunikačných entít opisujú nasledujúce články, aby sa doplnilo zdôvodnenie, prečo sa tieto veci označili ako potenciálne nové požiadavky.

5.2.5.5 Vytvorenie (registrácia) spôsobilosti bezpečného zasielania správ

5.2.5.5.1 Registrácia zariadenia

Článok opisuje kroky potrebné na vytvorenie spôsobilosti bezpečného zasielania správ medzi zdravotníckymi zariadeniami alebo aplikáciami a medzi týmito systémami a používateľmi. Zariadenia/aplikácia môžu obsahovať pacientove vyhradené zariadenie/aplikáciu dohliadajúce na zdravotný stav, poskytovateľov systém EMR atď. Používateľom môže byť pacient alebo poskytovateľ, alebo ich zástupca. Pozornosť v tejto časti sa venuje registrácii zariadenia. Registráciu používateľského zariadenia na zasielanie správ rieši nasledujúci článok.

Prednostne sa požadujú tieto kroky:

1. Pacientovo a poskytovateľovo zdravotné zariadenie/aplikácie sa nezávisle autentizujú a registrujú vo vrstve prvkov služby, ako aj vyhlasujú/potvrdzujú požiadavky na svoju triedu služby (a triedu zariadenia).

2. Ak je žiadosť platná, systémy sú autentizované a autorizované.

3. Vytvorí sa preklad názvu/adresy (kvôli smerovaniu) a plán činnosti sa zaznamená (v prípade, že zariadenie si vyžaduje prístup k sieti len podľa vopred stanoveného rozvrhu).

4. Zariadenie sa samo konfiguruje na základe nastavení určených používateľom alebo aplikáciou siete. V niektorých prípadoch môže byť potrebné zariadenie nakonfigurovať ručne.

Funkčné mapovanie uvedených krokov je nasledujúce:

a) Zariadenie/aplikácia M2M iniciuje žiadosť o registráciu.

b) Entita s vhodnou spôsobilosťou služby zostavuje spojenie a abstrahuje ho z aplikácií M2M a riadiacich funkcií.

c) Sieťový priechod M2M (ak sa použije) prenáša (smeruje) žiadosť o registráciu do siete (zriadi prístup k potrebným prvkom spôsobilostí v sieti).

d) Entita príslušného prvku služby registruje, overuje totožnosť a oprávňuje aplikácie M2M, a zabezpečuje konektivitu s inými prvkami spôsobilostí.

e) Entita s vhodnou spôsobilosťou služby sleduje a prihlasuje počiatočnú registráciu zariadenia alebo sieťového priechodu M2M.

f) Entita s vhodnou spôsobilosťou služby poskytuje meno na mapovanie sieťovej adresy a monitoruje stav zariadenia a „dosiahnuteľnosť".

g) Entita s vhodnou spôsobilosťou služby vyberá sieťové adresy z aplikácie M2M. Zabezpečuje aj výber siete (založený na triede služby a ďalších faktoroch) pre zariadenia, ktoré podporujú viac sietí alebo komunikačných služieb. Entita tiež zvažuje triedu služby zariadenia s cieľom výberu služieb siete a komunikácie.

h) Zariadenie a entita s vhodnou spôsobilosťou služby koordinujú správy, aby bolo možné správne nastaviť zariadenie na základe konkrétnej aplikácie a požiadaviek pacientov.

5.2.5.5.2 Registrácia používateľa

Článok opisuje kroky potrebné na vytvorenie spôsobilosti bezpečného zasielania správ medzi pacientom a poskytovateľom na komunikáciu používateľ-zariadenie alebo zariadenie-používateľ. Takáto komunikácia sa môže uskutočniť prostredníctvom aplikácie M2M, ktorá pracuje v centralizovanom systéme, štandardného internetového zariadenia (notebook, inteligentný telefón atď.), pomocou rozhrania založeného na webe alebo nejakým iným systémom bod-bod.

Prednostne sa požadujú takéto kroky:

1. Každý používateľ systému (pacient, poskytovateľ atď.) musí vykonať počiatočnú registráciu v aplikácii bezpečného zasielania správ.

2. Registrácia zahŕňa vytvorenie identity používateľa sústredením podrobných osobných údajov potrebných na bezpečnostné kontroly.

Funkčné mapovanie je nasledujúce:

a) Pred registráciou používateľa (prípadne počas registrácie zariadenia) vytvorí aplikácia M2M zoznam oprávnených používateľov pre zariadenia a aplikácie. Popri všeobecnom prístupe sa musí zaznamenať úroveň prístupu. Napríklad používateľ má oprávnenie prekonfigurovať zariadenie aj preto, aby dokázal z neho získať hodnoty atď. Tieto informácie sa ukladajú v entite so spôsobilosťou služby, ktorá zodpovedá za povolenie a zriadenie pripojenia k ostatným spôsobilostiam.

b) Používateľ iniciuje postup registrácie v rámci aplikácie bezpečného zasielania správ.

c) Používateľ poskytuje osobné údaje, aby sa vytvorila identita používateľa ako aj heslá a ďalšie bezpečnostné mechanizmy.

d) Identita používateľa sa porovná s oprávneným zoznamom používateľov v entite s vhodnou spôsobilosťou služby.

e) Entita potvrdzuje zariadenia a aplikácie, ku ktorým má používateľ oprávnený prístup, rovnako ako úroveň prístupu.

f) Informácia o prístupe používateľov a povolenom prístupe k zariadeniu/aplikácii sa ukladá do entity s vhodnou spôsobilosťou služby.

5.2.5.6 Prípady používania komunikácie (iniciované pacientom alebo poskytovateľom)

5.2.5.6.1 Komunikácia používateľ – zariadenie (inicializované používateľom)

Článok opisuje komunikáciu medzi používateľom (pacient alebo poskytovateľ) a zariadením alebo aplikáciou M2M. Príkladom tejto komunikácie sú poskytovatelia, ktorí žiadajú vzdialené monitorovacie zariadenie o namerané hodnoty, konfigurujúci takéhoto zariadenia, alebo pacient, aktualizujúci svoj EMR (alebo zdravotnú databázu) nejakými relevantnými informáciami.

Pri tomto type komunikácie sa vykonávajú nasledujúce kroky:

1. Poskytovateľ alebo pacient sa prihlási do systému bezpečného zasielania správ pomocou svojej identity používateľa a hesla (a iných bezpečnostných poverení).
2. Vyberú činnosť a zariadenie, ktoré majú spolu komunikovať (v niektorých prípadoch nemusia byť zariadenia v tom čase priamo pripojené).
3. Zadajú nové informácie alebo dopyt na zariadenie.
4. Aplikácia kontaktuje zariadenie s požiadavkou. To sa uskutoční v reálnom čase alebo neskôr, kedy je zariadenie „dostihnuteľné".
5. Odosielateľ informácie dostane správu o stave žiadosti a poskytne sa mu informácia (ak je k dispozícii).

Mapovanie funkcií je nasledujúce:

a) Entita bezpečného zasielania správ AAA (entita spôsobilosti služby) v sieti overuje a oprávňuje používateľa.

b) Entita s vhodnou spôsobilosťou služby zostavuje spojenie a abstrahuje ho z aplikácií M2M a riadiacich funkcií.

c) Správa sa vytvorí, vyšle a analyzuje sa sieťou kvôli identite prijímacieho zariadenia.

d) Entita s vhodnou spôsobilosťou služby potvrdí, že zariadenie je registrované, a vyhľadá mapovanie názvu na adresu siete. Zabezpečí aj výber siete (založený na triede služieb a ďalších ukazovateľoch) pre zariadenia, ktoré podporujú viac sietí alebo komunikačné služby.

e) Entita s vhodnou spôsobilosťou služby skontroluje aktuálny stav zariadenia (dosiahnuteľné alebo nie) a poslednú známu trasu.

f) Vhodná spôsobilosť služby môže tiež zabezpečiť spoplatňovanie záznamov na využitie spôsobilosti.

g) Entita s vhodnou spôsobilosťou služby monitoruje a zabezpečuje konfiguráciu, prevádzku a funkcie chybového manažérstva (sleduje výmenu správ z pohľadu chybovosti, porúch atď.).

h) Entita s vhodnou spôsobilosťou služby bude prenášať správy medzi aplikáciou bezpečného zasielania správ a zariadením M2M cez sieťový priechod M2M v prípade potreby. Spracuje retransmisie, hlási chyby, skrýva zbytočné informácie a monitoruje stav doručenia.

i) Entita s vhodnou spôsobilosťou služby uchováva kópie správ a stavu doručenia, chybové hlásenia atď.

j) Sieťový priechod M2M (ak platí) prenáša (alebo smeruje) správu do siete.

k) Zariadenie M2M prijme správu.

Entita s vhodnou spôsobilosťou služby aktualizuje odosielateľa správou o stave a požadovanými informáciami (ak to platí).

5.2.5.6.2 Komunikácia iniciovaná zariadením

Článok opisuje komunikáciu od zariadenia (alebo aplikácie) M2M k inému zariadeniu (alebo aplikácii) M2M alebo od zariadenia (alebo aplikácie) M2M k používateľovi.

Pri tomto type komunikácie sa vykonávajú nasledujúce kroky:

1. Podľa vopred určeného plánu alebo na základe nejakej udalosti sa zariadenie „prebudí" a zaregistruje sa v sieti, ak už nie je pripojené.

2. Ak sieť nie je k dispozícii, potom sa správa uloží a vykonajú sa pokusy o pripojenie na sieť vo vopred definovaných intervaloch.

3. Ihneď po pripojení je správa pripravená a odoslaná.

4. Správa sa doručí (ak doručenie zlyhá, skúša sa samostatná retransmisia).

5. Stav doručenia správy sa oznámi späť do odosielajúceho zariadenia M2M (alebo aplikácie).

Mapovanie funkcií je nasledujúce:

a) Nevyhnutný predpoklad: zariadenie M2M sa aktivuje a zaregistruje do siete (podrobne v predchádzajúcom článku).

b) Entita s vhodnou spôsobilosťou služby zostavuje spojenie a abstrahuje ho z aplikácií M2M a riadiacich funkcií.

c) Zariadenie M2M pripraví a vyšle správu.

d) Sieťový priechod M2M (ak platí) prenáša (smeruje) správu do siete.

e) Entita s vhodnou spôsobilosťou služby vykonáva smerovanie na spôsobilosti služby podľa potreby, a môže tiež zabezpečiť spoplatňovanie záznamov na využitie spôsobilosti.

f) Entita s vhodnou spôsobilosťou služby vyberie názov a informácie o pripojení z aplikácie M2M a funkcií manažérstva. Tiež monitoruje a zabezpečuje konfiguráciu, prevádzku a funkcie chybového manažérstva (sleduje výmenu správ z pohľadu chybovosti, porúch atď.).

g) Entita s vhodnou spôsobilosťou služby bude prenášať správy medzi zariadením M2M, sieťovým priechodom M2M a aplikáciou M2M (v sieti). Spracuje retransmisie, hlási chyby, skrýva zbytočné informácie a monitoruje stav doručenia.

6) Entita s vhodnou spôsobilosťou služby uchováva kópie správ a stavu doručenia, chybové hlásenia atď.

h) Aplikácia M2M (zariadenie alebo sieťová doména) prijme správy.

Je potrebné poznamenať, že existuje požiadavka, aby služby siete alebo aplikačnej domény boli vždy k dispozícii. Zariadenia sa nemusia vždy pripojiť a preto možno požadovať ukladanie, smerovanie dopredu a podobné techniky na zabezpečenie distribúcie správ a na potvrdzovanie.

5.2.5.7 Údržba zariadenia

5.2.5.7.1 Aktualizácia softvéru

Článok opisuje požiadavky na aktualizáciu softvéru alebo vykonávanie iných typov postupov údržby zariadení M2M. To predpokladá, že zariadenie má schopnosť podporovať aktualizáciu typu „vzdušného prenosu" prostredníctvom prístupovej technológie zariadenia. Ďalej sa predpokladá, že zariadenie má schopnosť ukladať záložnú verziu softvéru a môže „vrátiť späť" softvér, ak by bol problém s novou aktualizáciou.

Pri tejto činnosti sa vykonávajú nasledujúce kroky:

1. Sieť uvádza, že zariadenia majú dostupnú aktualizáciu softvéru.
2. Zariadenie signalizuje, že je dostupná aktualizácia softvéru.
3. V závislosti od nastavenia konfigurácie zariadenia aktualizácia softvéru sa môže vykonať automaticky alebo môže požiadať používateľa/vlastníka zariadenia, aby povolil aktualizáciu.
4. Sieť iniciuje aktualizáciu softvéru zariadenia. Platnosť tohto softvéru musí potvrdiť zariadenie predtým, kým sa povolí začatie aktualizácie.
5. Prístroj sa reštartuje a začne používať nový softvér.

Mapovanie funkcií je nasledujúce:

a) Entita s vhodnou spôsobilosťou služby, ktorá je zodpovedá za správu konfigurácie, dostane upozornenie, že na zariadenie je dostupná aktualizácia softvéru. Možno ju vykonať prostredníctvom stanoveného postupu medzi prevádzkovateľom siete a dodávateľom zariadenia/aplikácie.

b) Entita s vhodnou spôsobilosťou služby vytvorí spojenie so zariadením a odošle zariadeniu správu, že je dostupná aktualizácia softvéru.

c) Zariadenie aktualizáciu softvéru prijme, odmietne alebo odloží spôsobom stanoveným v nastaveniach konfigurácie zariadenia (automatická aktualizácia, ponúknutá aktualizácia atď.).

d) Ihneď po prijatí aktualizácie zariadením entita so spôsobilosťou služby stiahne aktualizáciu do zariadenia.

e) Zariadenie overí, že aktualizácia softvéru je platná a schválená vhodnými bezpečnostnými opatreniami (entita so spôsobilosťou služby v sieti zodpovedá za uplatňovanie bezpečnostných mechanizmov pri preberaní softvéru).

f) Hneď ako sa sťahovanie dokončí, prístroj sa reštartuje a začne používať nový softvér.

Po reštarte sa prístroj znovu zaregistruje do siete a potvrdí svoje požiadavky na triedu služby a konfiguráciu.

5.3 Meranie signálov tela s veľmi nízkym napätím (MVLBS)

5.3.1 Všeobecný opis

V scenári diaľkového dohľadu nad pacientom, pri ktorom je potrebné získať nízkonapäťové signály tela, aby sa dosiahli požadované ciele diaľkového dohľadu nad zdravotným stavom, môže postup získavania v skutočnosti rušiť rádiový prenos, napríklad GSM/GPRS, ktorý môže prebiehať v najbližšom okolí umiestnených rádiových častí toho istého zariadenia M2M.

V prípade nepretržitého sledovania zdravotného stavu pacienta, napríklad pri zisťovaní arytmie, by získavanie údajov mohla rušiť typická činnosť pri komunikácii bunkových rádií vykonávaná v zariadení M2M.

Je veľmi dôležité, aby sa zabránilo alebo znížilo možné rušenie prichádzajúcich signálov tela, aby sa dosiahla spoľahlivá elektronická zdravotná služba, aj keď nemá charakter záchrannej služby.

Spôsob, ako sa vyrovnať s neočakávaným rušením rádiového vysielania, je súčasné vzorkovanie rádiového prenosového signálu s cieľom upraviť postup vzorkovania signálu zameraný na znižovanie rušivých vplyvov, napríklad zrušením alebo opravením tých prijatých vzoriek, ktoré tvoria aktívnu časť rádiového vysielania, alebo mierne posunutie času vzorkovania signálu. Ďalším spôsobom môže byť riadenie rádiového vysielača prerušením rádiového prenosu na vymedzený čas merania, a potom jeho obnovenie po ukončení relácie merania.

5.3.2 Zainteresované subjekty

Zainteresované subjekty sú rovnaké ako v prípade používania diaľkového dohľadu nad pacientom.

5.3.3 Postup

Postup je rovnaký ako v prípade použitia diaľkového dohľadu nad pacientom ale na získavanie signálov tela s veľmi nízkym napätím sa používa vzdialené monitorovacie zariadenie.

5.3.4 Výmena informácií

Výmena informácií je rovnaká ako v prípade používania diaľkového dohľadu nad pacientom.

5.3.5 Potenciálne nové požiadavky

5.3.5.1 Elektronické zdravotnícke pomôcky bez rušenia

Systém M2M alebo jeho časti majú zabrániť rušeniu, ktoré vzniká pri detegovaní a meraní signálov veľmi nízkeho napätia, aby ich mohli získať a používať aplikácie M2M (napríklad v prípade aplikácií elektronického zdravotníctva, kde signály tela EKG, ktoré sa nepretržito merajú sieťou bezdrôtových senzorov tela, môžu intenzívne rušiť najbližšie vysielače GSM/GPRS, ktoré patria k sieťovému priechodu M2M elektronickej zdravotníckej pomôcke).

5.3.5.2 Indikácia činnosti rádiového vysielania

V závislosti od typu služby M2M všetky časti rádiového vysielania (napríklad GSM/GPRS) zariadenia (alebo sieťového priechodu) M2M musia zabezpečiť v reálnom čase indikáciu činnosti rádiového vysielania k aplikácii v zariadení/sieťovom priechode M2M.

5.3.5.3 Riadenie činnosti rádiového vysielania

V závislosti od typu služby M2M aplikácia v zariadení/sieťovom priechode M2M môže dať v reálnom čase pokyn všetkým častiam rádiového vysielania (napríklad GSM/GPRS) v zariadení (alebo sieťovom priechode) M2M, aby prerušili/pokračovali v činnosti rádiového vysielania.

5.4 Prenos dát pri starostlivosti na diaľku medzi domácnosťou a vzdialeným monitorovacím centrom

5.4.1 Všeobecný opis

Prípad používania sa zaoberá poskytnutím komunikačného vedenia IP na prenos dát pri starostlivosti na diaľku (poplachy, výber dát, sledovanie udalostí životného štýlu) a dvojcestnou hlasovou komunikáciou medzi domácnosťou a vzdialeným monitorovacím centrom, ktorá zabezpečuje vzájomnú spoluprácu medzi rôznymi zariadeniami v domácnosti určenými na starostlivosť na diaľku a riešeniami vzdialeného monitorovacieho centra.

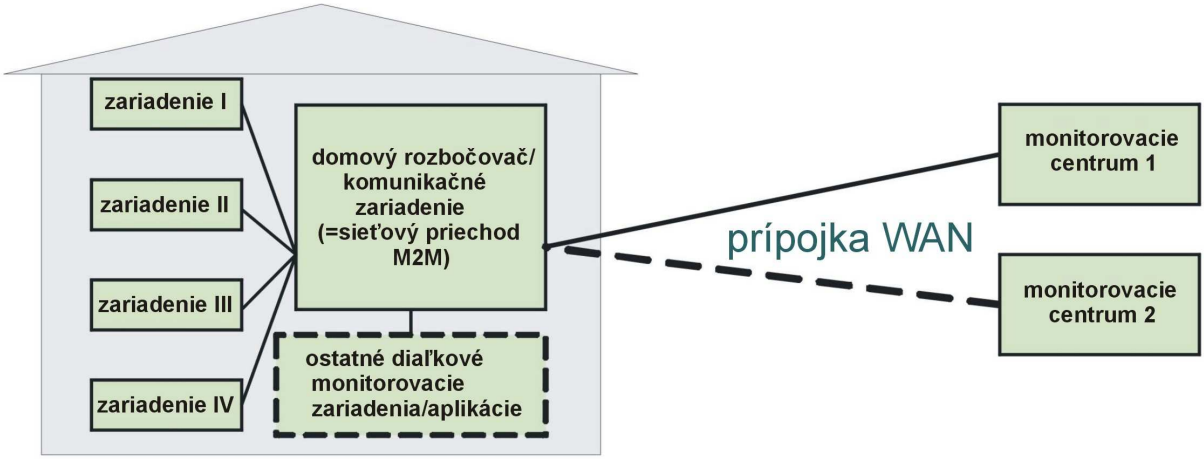
Je potrebné venovať osobitnú pozornosť bezpečnosti a ochrane súkromia, pretože spojenie používa informácie, ktoré by sa mohli využiť na identifikáciu zraniteľných jedincov.

5.4.2 Zainteresované subjekty

Prípad používania zahŕňa nasledujúce zainteresované subjekty:

- spotrebiteľ;
- pracovník monitorovacej služby;
- technik monitorovacej služby/technik inštalácie;
- poskytovateľ starostlivosti.

5.4.3 Scenár



Obrázok 2 – Základný postup tohto prípadu používania

Prenos väčšiny údajov pri starostlivosti na diaľku bude potrebný, aby sa podporili kritické situácie s poplachom v reálnom čase. Situácie s poplachom obyčajne začínajú telefonickým volaním. V týchto poplachových situáciách je hlavným kritériom dostupnosť a spoľahlivosť spojenia (možno vyžadujúce núdzové riešenia).

Niektoré dáta pri starostlivosti na diaľku nemožno považovať za rozhodujúce v reálnom čase (napríklad dáta s dávkou každodenných činností, informácie o konfigurácii pripomienky a pod.), ktoré sa môžu uložiť a odovzdať neskôr, ak spojenie nie je k dispozícii.

Stále viac systémov môže generovať aj významné „technické" senzory skúmajúce prevádzku, aby sa presvedčili, že sú stále aktívne, požadujúce stav dobitia batérie atď. Veľa z uvedeného sa uskutoční v rámci prevádzky vo WAN.

Prípad používania vyžaduje vyvinúť úsilie na schválenie požiadavky a špecifikácie na otvorený protokol na prenos oboch uvedených kategórií dát cez dátové spoje IP pomocou M2M SCL.

Prípad používania sa zaoberá otázkami interoperability, ktoré súvisia s rozhraním WAN medzi domovým rozbočovačom (= sieťový priechod M2M) alebo ekvivalentným osobným komunikačným zariadením a monitorovacím centrom.

Rozsah tohto prípadu používania možno rozdeliť do dvoch oblastí:

1. Pripojiteľnosť IP a definícia správy v prípade poplachov a riadeného zasielanie správ pomocou WAN.
2. Pripojiteľnosť IP, aby obsahovala stríming hlasových a iných interaktívnych strímingových dát v reálnom čase.

Typický postup

Je zrejmé, že veľká časť práce, ktorú treba vykonať v týchto príkladoch, nezávisí od domény starostlivosti na diaľku. Alebo inými slovami, vykonaná primárna práca nezávisí od užitočného zaťaženia.

Séria noriem IEEE 11073 [i.1] na zariadenia, ktoré sa nachádzajú v mieste poskytnutia zdravotnej starostlivosti, pravdepodobne predstavuje dobrý východiskový bod na rozvoj globálne použiteľných dátových noriem na rozhranie, v nadväznosti na normy, ktoré v súčasnej dobe stanovuje BS 8521 [i.2] a ďalšie široko používané vlastnícke formáty.

V mnohých prípadoch sa očakáva, že domový rozbočovač bude minimálne spracúvať dáta zo zariadení.

Aj napriek tomu, že užitočné dáta sa zobrazujú všeobecne, je stále ešte užitočné rozdeliť prenos dát na päť základných typov:

- epizodický – dáta jednej asynchrónnej udalosti;
- stríming – nepretržitý tok dát v reálnom čase;
- dokument – ľubovoľne veľký súbor dát;
- riadenie – posielaná správa, ktorá prikazuje príjemcovi zmeniť svoje správanie ;
- poplachy – posielaná správa, ktorá obsahuje rôzny stupeň naliehavosti.

Touto kategorizáciou sa rozčleňuje problém, pretože mechanizmy vybrané na presun užitočných dát majú zodpovedať základným potrebám každej kategórie.

Typy dát sa majú mapovať do komunikačných prostriedkov, ktoré potrebujú zodpovedajúce vlastnosti QoS pri každom dátovom type (napríklad použitie vhodných tried služby M2M).

Nasleduje formátovanie, ktoré prípad používania ukladá na možné riešenia.

V prípade poruchy (napríklad poruchy nejakého externého rozhrania WAN, degradácie, zníženia šírky pásma, zistený požiar):

- zabezpečí sa vysoká odolnosť pri prenose poplachových informácií;
- žiadne dáta sa nestratia (potenciálne všetky typy dát alebo len poplachové dáta a niektoré lekárske dáta);
- na vyžiadanie (napríklad aplikáciami, poplachmi, ľudskou interakciou) sa umožní údržba hlasových služieb podľa prijatých noriem výkonnosti.

Musí sa pracovať súčasne s normálnym súborom „domácich" služieb založených na IP, ktoré fungujú pomocou rovnakého širokopásmového pripojenia (automatizácia domácnosti, zábava atď. rovnako ako ostatné diaľkové monitorovacie služby, ako diaľkové zdravotnícke služby).

Vonkajšia závislosť: domový rozbočovač musí dokázať naďalej zasielať poplachové signály do monitorovacieho centra v prípade zlyhania napájania v objekte.

5.4.4 Výmeny informácií

1. Domový rozbočovač (=sieťový priechod M2M) k vzdialenému monitorovaciemu centru:

Zásadne je tento tok určený na distribúciu dát, ktoré obsahuje domový rozbočovač, k ľubovoľnému monitorovaciemu centru pomocou rozhrania WAN. Presné kroky, ako to dosiahnuť, by určoval podrobný vývoj aplikácie, ktorou sa implementuje tento prípad používania, ale pravdepodobne by sa vychádzalo z nasledujúceho:

– domový rozbočovač má dáta určené na komunikáciu so vzdialeným monitorovacím centrom; tieto dáta prichádzajú pravdepodobne z pripojených zariadení, ale môže ísť aj o iné údaje; môže to predstavovať jeden dátový bod alebo súbor mnohých dátových bodov;

– dáta sa rozšírili; podrobnosti budú opäť závisieť od konkrétnej aplikácie použitej pri realizácii príkladu tohto prípadu používania, ale to znamená rozširovať dáta niektorými ďalšími údajmi, napríklad ID zariadenia, časová pečiatka, ID používateľa alebo inými potrebnými relevantnými údajmi pre tento tok;

– dáta sú pripravené na prenos; údaje sa môžu konvertovať (informačný model alebo formát); potom by sa stanovilo požadované zabezpečenie a ochrana osobných údajov (požadované zabezpečenia sa môžu vykonať aj v aktuálnom prenose);

– dáta sa vyšlú;

– potvrdenie o úspešnom prijatí dát vo vzdialenom monitorovacom centre.

2. Vzdialené monitorovacie centrum k domovému rozbočovaču:

Obvykle je tok určený na distribúciu prevádzky s nízkou hlasitosťou, ako sú dáta s príkazmi zo vzdialeného monitorovacieho centra k domovému rozbočovaču pomocou rozhrania WAN. Presné kroky, ako to dosiahnuť, by určovala podrobná príprava aplikácie, ktorou sa implementuje prípad používania, ale pravdepodobne by sa vychádzalo z nasledujúceho:

– vzdialené monitorovacie centrum má dáta s príkazmi určené na komunikáciu s domovým rozbočovačom; príkaz môže používať domový rozbočovač alebo ho môžu v konečnom dôsledku používať zariadenie pripojené k domovému rozbočovaču;

– dáta sa rozšírili; podrobnosti budú opäť závisieť od konkrétnej aplikácie použitej pri realizácii príkladu tohto prípadu používania, ale to znamená rozširovať dáta niektorými ďalšími údajmi, napríklad ID vzdialeného monitorovacieho centra, časová pečiatka, ID cieľového domáceho rozbočovača alebo inými potrebnými relevantnými údajmi pre tento tok;

– dáta sú pripravená na prenos; údaje sa môžu konvertovať (informačný model alebo formát); potom by sa stanovilo požadované zabezpečenie a ochrana osobných údajov (požadované zabezpečenia sa tiež musia vykonať pri prenose);

– dáta sa vyšlú;

– potvrdenie o úspešnom prijatí dát domovým rozbočovačom sa vráti do vzdialeného monitorovacieho centra.

5.4.5 Potenciálne nové požiadavky

Nasledujúci zoznam sumarizuje kandidátov na prípadné nové požiadavky:

- systém M2M má byť spôsobilý spracovávať prevádzku M2M v rôznych kategóriách (t. j. s rôznymi prioritami a s rôznymi charakteristikami);
- systém M2M má byť spôsobilý podporovať aplikácie, aby zostavil dvojcestnú hlasovú komunikáciu na žiadosť aplikácií a podľa priority prevádzky;

- systém M2M má byť spôsobilý podporovať aplikácie, aby zostavil inú interaktívnu komunikáciu v reálnom čase alebo komunikáciu so strímingom v reálnom čase (napríklad videa) na žiadosť aplikácií a príslušne priorizovať prevádzku;
- v prípade poruchy komunikačných spojov (čiastočná strata spojenia, pokles v kvalite, potreba prepnutia na zálohovanie atď.):

  – zabezpečí sa vysoká odolnosť pri prenose poplachových informácií;

  – zabráni sa strate dát (potenciálne všetkých typov alebo len dát týkajúcich sa poplachu a niektorých lekárskych údajov);

  – povolia sa hlasové služby, aby sa udržiavali podľa prijatých prevádzkových noriem;
- musí dokázať pracovať súčasne s normálnym súborom „domácich" súvisiacich služieb IP, ktoré fungujú pomocou rovnakého pripojenia (automatizácia domácnosti, zábava atď. rovnako ako ostatné diaľkové monitorovacie služby, ako diaľkové zdravotnícke služby);
- vonkajšia závislosť: domový rozbočovač musí byť schopný naďalej zasielať poplachové signály do monitorovacieho centra v prípade zlyhania napájania v objekte.

História

História dokumentu		
V1.1.1	September 2013	Publikácia