ETSI TS 102 689 V1.1.1 (2010-08)

Technická špecifikácia

Komunikácia stroj-stroj (M2M);
Požiadavky na službu M2M

Machine-to-Machine communications (M2M);
M2M service requirements

Európsky inštitút pre telekomunikačné normy

European Telecommunications Standards Institute

Referenčné číslo

DTS/M2M-00001

Kľúčové slová

M2M, service

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://www.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

Práva duševného vlastníctva, ktoré majú alebo môžu mať zásadný význam pre tento dokument, mohli byť oznámené 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 SR 000 314 s názvom Práva duševného vlastníctva (IPRs); Zásadné alebo potenciálne zásadné práva duševného vlastníctva, oznámené organizácii ETSI vo vzťahu k normám ETSI, ktorý je možno získať na sekretariáte ETSI. Najnovšie znenie je dostupné na serveri ETSI http://www.etsi.org/ipr.

V súlade so svojou politikou v oblasti práv duševného vlastníctva ETSI neskúma ani nevyhľadáva žiadne práva duševného vlastníctva. Neposkytuje ani záruku na iné práva duševného vlastníctva, ktoré nie sú uvedené 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 špecifikáciu (TS) navrhla technická komisia ETSI Komunikácia stroj – stroj“ (M2M).

Úvod

Komunikácia stroj – stroj (M2M) je komunikácia medzi dvomi alebo viacerými jednotkami, ktoré nepotrebujú žiadny ľudský zásah. Služby M2M sú určené na automatické rozhodovanie a spracovanie komunikácie.

Požiadavky služby M2M uvedené v tomto dokumente umožnia konzistentnú, nenákladnú, komunikáciu v širokom rozsahu všadeprítomných aplikácií. Príklady takýchto aplikácií obsahujú: ľahké manažérstvo, inteligentné meranie, automatizáciu domácnosti, elektronické zdravotníctvo a pod.

V dokumente, spolu so špecifikáciou architektúry v TS 102 690 [i.1], sú vytvorené základy na podrobné technické špecifikácie komunikácie M2M.

V dokumente sú špecifikované všeobecné a funkčné požiadavky na komunikačné služby M2M.

1 Predmet

V dokumente sa špecifikujú požiadavky na služby M2M zamerané na efektívne doručenie služieb M2M medzi koncovými bodmi.

Dokument obsahuje nasledovné články:

- **všeobecné požiadavky** – opisujú funkcie komunikácie potrebné na presné vytvorenie komunikácie M2M;
- **manažment** – špecifikuje požiadavky súvisiace s riadiacimi režimami (detekcia chybných funkcií, konfigurácia, spoplatnenie, a pod.);
- **funkčné požiadavky na služby M2M** – opisujú požiadavky funkcií M2M (zber a vykazovanie dát, diaľkové kontrolné činnosti a pod.);
- **bezpečnosť** - obsahuje požiadavky na overovanie totožnosti zariadení M2M, na integritu dát, súkromie a pod;
- **identifikátory, číslovanie a adresovanie** – poskytuje požiadavky týkajúce sa spôsobov identifikácie, číslovania a adresovania špecifických M2M.

Požiadavky M2M v tomto dokumente sú ovplyvnené nasledovnými prípadmi použitia:

- prípady použitia inteligentných meračov opísané v TR 102 691 [i.2];
- prípady použitia elektronického zdravotníctva opísané v TR 102 732 [i.3];
- prípady použitia sledovania a vyhľadávania opísané v prílohe B;
- prípady použitia monitorovania opísané v prílohe B;
- prípady použitia transakcie opísané v prílohe B;
- prípady použitia kontroly opísané v prílohe B;
- prípady použitia automatizácie domácností opísané v prílohe B;
- prípady použitia automatizácie mesta opísané v TR 102 897 [i.4];
- prípady použitia pripojených účastníkov opísané v TR 102 875 [i.5];
- prípady použitia automobilov opísané v TR 102 898 [i.6].

2 Referenčné dokumenty

Referenčné dokumenty sú špecifikované (určené dátumom vydania, číslom vydania, číslom verzie atď.), alebo nešpecifikované. V prípade špecifikovaného referenčného dokumentu sa použijú len uvedené verzie. Pri nešpecifikovanom referenčnom dokumente sa použije posledná verzia referenčného dokumentu (vrátane akýchkoľvek dodatkov).

Uvádzané referenčné dokumenty, ktoré nie sú verejne dostupné na predpokladanom mieste sa môžu vyhľadať na http://docbox.etsi.org/Reference.

> POZNÁMKA. – Pokiaľ akýkoľvek odkaz uvedený v tejto kapitole bol platný v čase publikovania, ETSI nemôže garantovať jeho platnosť z dlhodobého hľadiska.

2.1 Normatívne referenčné dokumenty

Dokumenty sú nevyhnutné v špecifikácii.

Nepoužívajú sa.

2.2 Informatívne referenčné dokumenty

Dokumenty nie sú dôležité v technickej špecifikácii, ale pomáhajú používateľovi v konkrétnej predmetnej oblasti.

[i.1] ETSI TS 102 690 :"Machine-to-Machine communications (M2M); M2M functional architecture".

[i.2] ETSI TR 102 691: "Machine-to-Machine communications (M2M); Smart Metering Use Cases".

[i.3] ETSI TR 102 732: "Machine to Machine Communications (M2M); Use cases of M2M applications for eHealth".

[i.4] ETSI TR 102 897: "Machine to Machine Communications (M2M); Use cases of M2M applications for City Automation".

[i.5] ETSI TR 102 875: "Access, Terminals, Transmission and Multiplexing (ATTM); Study of European requirements for Virtual Noise for ADSL2, ADSL2plus and VDSL2".

[i.6] ETSI TR 102 898: "Machine to Machine Communications (M2M); Use cases of Automotive Applications in M2M capable networks".

[i.7] ISO 16750: "Road vehicles -- Environmental conditions and testing for electrical and electronic equipment".

[i.8] ETSI TS 102 412: "Smart Cards; Smart Card Platform Requirements Stage 1 (Release 8)".

3 Skratky

V dokumente sa používajú skratky:

AEC	Automotive Electronics Council	výbor pre automobilovú elektroniku
CO	Connected Object	spojený objekt
CPE	Customer Premises Equipment	zariadenie v priestoroch zákazníka
EPOS	Electronic Point of Sale	elektronický platobný terminál
HLR	Home Location Register	register domácich účastníkov
HSS	Home Subscriber Server	domáci účastnícky server
IMSI	International Mobile Subscriber Identity	medzinárodná identita pohyblivého účastníka
M2M	Machine-to-Machine (communication)	komunikácia stroj-stroj
MVNP	Mobile Virtual Network Operator	prevádzkovateľ virtuálnej mobilnej siete
NAT	Network Address Translator	prekladač sieťovej adresy
PLC	Power Line Communication	komunikácia po elektrickom vedení
QoS	Quality of Service	kvalita služby
RFID	Radio Frequency IDentification	rádiofrekvenčná identifikácia
SLA	Service Level Agreement	zmluva o úrovni služby
TrE	Trusted Environment	dôveryhodné prostredie
UICC	Universal Integrated Circuit Card	univerzálna karta s integrovaným obvodom
WAN	Wide Area Network	rozsiahla počítačová sieť

4 Všeobecné požiadavky

Všeobecné požiadavky špecifikované ďalej v systéme M2M všeobecne znamenajú, že nie všetky osobitné systémy M2M alebo prvky týchto systémov potrebujú realizovať každú požiadavku.

Systém M2M musí podporovať nastavenie rozličných kategórií služby, podľa TS 102 690 [i.1].

To znamená až k riadiacej sieti M2M kontrolovať párovanie medzi kategóriou služby, požadovanou aplikáciou M2M a vlastnosťami zariadenia. Ak sa nájde nezhoda, riadiaci systém M2M musí vyslať upozornenie k aplikácii M2M. Aplikácia M2M musí umožniť požiadavku vlastností zariadenia.

4.1 Princípy komunikácie aplikácie M2M

Systém M2M musí umožniť komunikáciu medzi aplikáciami M2M v sieti a doménami aplikácií a zariadením M2M alebo sieťovým priechodom M2M, použitím viacnásobných komunikačných prostriedkov, napríklad SMS, GPRS a prístupu IP.

Aj spojené objekty môžu komunikovať spôsobom partner – partner s akýmkoľvek iným spojeným objektom.

Systém M2M musí mať funkcionalitu začlenenia používanej sieťovej štruktúry vrátane akéhokoľvek používaného spôsobu adresovania, napríklad v prípade siete IP zostavenie relácie sa musí umožniť, ak sa použije statické alebo dynamické adresovanie IP.

> POZNÁMKA. – Abstrakcia (napríklad, prevádzkového prostredia a topológie) siete môže znížiť úsilie pri vývoji aplikácie v rozličných variantoch.

4.2 Doručovanie správ zariadeniam v pohotovostnom stave

Systém M2M musí mať funkcionalitu riadenia komunikácie so zariadeniami v pohotovostnom stave.

4.3 Režimy doručovania

Systém M2M musí podporovať komunikačné režimy rezervovaného vysielania, individuálneho vysielania, skupinového vysielania a globálneho vysielania. Ak je to možné globálne vysielanie sa musí nahradiť skupinovým vysielaním alebo individuálnym vysielaním pri zníženej záťaži v komunikačnej sieti.

4.4 Plánovanie prenosu správ

Systém M2M musí mať funkcionalitu riadenia plánovania prístupu k sieti a prenášanie správ.

Systém M2M musí mať prehľad o plánovaní tolerancie oneskorenia aplikácie M2M.

4.5 Výber komunikačnej trasy správy

Systém M2M musí mať funkcionalitu optimalizácie komunikačných tras, založenú na stratégii nákladov v sieti, oneskorení alebo prenosových porúch, ak existujú iné komunikačné trasy.

4.6 Komunikácia so zariadeniami za sieťovým priechodom M2M

Systém M2M musí mať funkcionalitu komunikácie so zariadeniami za sieťovým priechodom M2M.

4.7 Hlásenie porúch v komunikácii

Aplikácie M2M, požadujúce dôveryhodné doručenie správy, musia mať informácie o akýchkoľvek poruchách doručenia správy.

4.8 Modularita

Systém M2M musí byť modulárny vzhľadom na počet spojených objektov.

4.9 Zahrnutie heterogénnych technológií

Systém M2M musí umožňovať spojenia k rozličným technológiám miestnej siete M2M.

4.10 Vlastnosti služby – funkcionality vyhľadávania a registrácie

Systém M2M musí podporovať spôsob umožňujúci aplikáciám M2M zistiť vlastnosti služby M2M, ktoré sa im ponúkajú.

Zariadenie M2M a sieťový priechod M2M musia podporovať spôsoby umožňujúce registráciu vlastností svojich služieb v systéme M2M.

4.11 Zabezpečené aplikácie M2M

Riadiaci systém M2M môže spracovať odpoveď na požiadavku služby zabezpečených aplikácií pomocou moderných postupov overovania totožnosti.

Systém môže podporovať zabezpečené aplikácie. Sú to aplikácie vopred schválené riadiacim systémom M2M.

Riadiaci systém M2M môže spracovať potvrdenia požiadavky služby spoľahlivých aplikácií M2M umožnením racionálnych postupov overovania totožnosti týchto aplikácie.

Systém M2M môže podporovať spoľahlivé aplikácie, čo sú aplikácie vopred schválené riadiacim systémom M2M.

4.12 Mobilita

Ak základná sieť podporuje bezpečnú mobilitu a rouming, systém M2M musí používať takéto mechanizmy.

4.13 Integrita komunikácie

Systém M2M musí podporovať mechanizmus na zaistenie integrity komunikácií v službách M2M.

4.14 Kontrola integrity zariadenia/sieťového priechodu

Systém M2M musí podporovať kontrolu integrity zariadenia M2M a sieťového priechodu M2M.

4.15 Trvalé spojenie

Systém M2M musí podporovať trvalé spojenie na aplikácie M2M požadujúce rovnakú službu M2M na pravidelnom a trvalom základe. Trvalé spojenie sa môže deaktivovať po požiadavke aplikácie alebo vnútorného mechanizmu v riadiacom systéme M2M.

4.16 Potvrdenie správ

Systém M2M musí podporovať mechanizmus potvrdenia správ. Správy nemusia byť potvrdené, môžu byť potvrdené alebo prenosom kontrolované.

4.17 Priorita

Systém M2M musí podporovať riadenie úrovní priority služieb a komunikačných služieb. Prebiehajúca komunikácia sa môže prerušiť pri obsluhe toku s vyššou prioritou (napríklad prednosť uvoľnenia).

4.18 Prihlásenie

Prenášaná správa transakcie požadujúca neodmietnutie musí mať funkcionalitu registrácie. Dôležité udalosti (napríklad prijatá informácia zo zariadenia M2M alebo sieťového priechodu je chybná, pokus o neúspešnú inštaláciu zo zariadenia M2M alebo sieťového priechodu M2M, služba nie je v činnosti a pod.) môžu sa registrovať spolu s diagnostickými informáciami. Registrácia sa musí obnoviť na požiadanie.

4.19 Anonymita

Systém M2M musí podporovať anonymitu. Ak aplikácia M2M požaduje anonymitu zo strany zariadenia M2M a požiadavku akceptuje sieť, sieťová infraštruktúra bude zatajovať identitu a lokalitu žiadateľa, podľa regulačných požiadaviek.

4.20 Časová pečiatka

Systém M2M musí podporovať presné, bezpečné a spoľahlivé časové pečiatkovanie. Zariadenia M2M a sieťové priechody M2M môžu podporovať presné, bezpečné a spoľahlivé časové pečiatkovanie.

4.21 Odolnosť proti poruchám zariadení/sieťových priechodov

Po nedeštruktívnej poruche, napríklad po výpadku napájacieho napätia, zariadenie alebo sieťový priechod M2M sa musia okamžite automaticky vrátiť do úplného prevádzkového stavu, po vykonaní príslušnej inicializácie, napríklad ak je podporovaná kontrola integrity.

4.22 Indikácia a kontrola aktivity rádiového prenosu

Rádiové prenosové časti (napríklad, GSM/GPRS) zariadenia/sieťového priechodu M2M musia poskytovať (ak sa požaduje osobitnou aplikáciou napríklad, e-zdravotníctvo) indikáciu rádiovej prenosovej aktivity v reálnom čase na aplikáciu na zariadení/sieťovom priechode M2M, a môže sa riadiť v reálnom čase aplikáciou na zariadení/sieťovom priechode M2M na zrušenie/pokračovanie rádiovej prenosovej aktivity.

4.23 Vystavenie vlastnostiam prevádzkovateľa siete

Rozhranie M2M k externým aplikáciám M2M musí oprávňovať vystaviť vlastnostiam prevádzkovateľa siete (e.g. SMS, USSD, lokalizácia, konfigurácia predplatného, overovanie totožnosti (napríklad všeobecná zavádzacia architektúra), a pod.). Platforma služby musí poskytovať prístup k prostriedkom mimo M2M zahrnutým medzi prostriedky M2M na poskytovanie aplikácie konzistentného použitia vlastností M2M (napríklad vyslať SMS k spoločným bunkovým telefónom).

4.24 Podpora hlásenia lokalizácie

Systém M2M musí oznamovať lokalitu zariadenia/sieťového priechodu M2M k aplikáciám M2M, ak je táto informácia dostupná. Informácia o lokalite zariadenia M2M/sieťového priechodu M2M sa môže určiť procedúrami základnej siete (s uvažovaním príslušného nastavenia súkromia/bezpečnosti na prenos takej informácie), informáciou na aplikačnej úrovni hlásenou aplikáciou zariadenia/sieťového priechodu M2M alebo kombináciou obidvoch.

4.25 Podpora viacerých aplikácií M2M

Systém M2M musí podporovať mechanizmus riadenia viacnásobných aplikácií M2M a poskytovať mechanizmus na spoluprácu medzi viacnásobnými aplikáciami M2M. Tento mechanizmus musí podporovať:

- udržiavanie zoznamu registrovaných aplikácií M2M;
- udržiavanie informácie o registrácii aplikácií M2M;
- potvrdenie novo registrovaných aplikácií M2M k predplateným aplikáciám M2M overených a oprávnených na výmenu informácií.

5 Manažérstvo

5.1 Poruchové manažérstvo

5.1.1 Preventívne monitorovanie

Systém M2M musí riadiť monitorovanie systému M2M s možnosťou ochrániť a opraviť chyby.

5.1.2 Režim diagnostiky

Systém M2M musí poskytnúť prostriedky na diagnostikovanie fungovania aplikácie M2M.

5.1.3 Skúška spojenia

Systém M2M musí podporovať skúšanie spojenia smerom k vybratému súboru pripojených objektov (CO) v pravidelných intervaloch poskytujúcich CO podporu funkcií.

5.1.4 Vyhľadávanie a hlásenie porúch

Prevádzkový stav spojeného objektu (CO) poskytnutý funkciou CO sa musí dať monitorovať.

5.1.5 Diaľkové riadenie obnovy po poruche

Zariadenia M2M môžu podporovať diaľkové riadenie na obnovu po poruche, napríklad aktualizáciou firmvéru, garantovaného zariadením. Po tejto činnosti aktualizácie firmvéru, zariadenie sa môže znovu nastaviť do známeho a konzistentného stavu.

5.1.6 Monitorovanie zmluvy o úrovni služby (SLA)

Zariadenia M2M a sieťové priechody M2M, ktoré podporujú monitorovanie SLA môžu zaznamenať napríklad výpadky napájania (vrátane trvania, času začatia a ukončenia) a komunikačné výpadky (vrátane trvania straty spojenia, času začatia a ukončenia).

5.2 Konfiguračné manažérstvo

5.2.1 Zriadenie a automatická konfigurácia zariadení a sieťových priechodov M2M

Aplikácie alebo vlastnosti M2M vo vlastnostiach služby musia podporovať automatickú konfiguráciu, ktorá je bez ľudského zásahu, zariadení M2M alebo sieťových priechodov M2M ak sú zapojené. Zariadenie M2M alebo sieťový priechod M2M môžu podporovať automatickú konfiguráciu a registráciu funkcií aplikácií M2M.

Systém M2M musí podporovať mechanizmus na vykonávanie jednoduchého a modulárneho mechanizmu zriadenia, ktorý musí pracovať aj keď komunikačná trasa k zariadeniu/sieťovému priechodu M2M chýba.

5.2.2 Zálohovanie miestnej siete M2M

Porucha zaznamenaná zariadením M2M alebo sieťovým priechodom M2M nesmie ovplyvniť normálnu činnosť miestnej siete M2M.

5.2.3 Časová synchronizácia

Systém M2M musí podporovať časovú synchronizáciu. Zariadenia M2M a sieťové priechody M2M môžu podporovať časovú synchronizáciu. Úroveň presnosti a bezpečnosti časovej synchronizácie môžu byť špecifické v systéme.

5.2.4 Konfiguračné manažérstvo

Systém M2M a sieťové priechody M2M musia podporovať konfiguračné manažérstvo (napríklad, schopnosť manažovania bude závislá na koncovom systéme).

5.3 Správa systému

5.3.1 Spoplatňovanie

Systém M2M musí podporovať generovanie informácie o spoplatnení použitia prostriedkov M2M.

5.3.2 Kompenzačné mechanizmy

Systém musí podporovať mechanizmus požadovaný na bezpečné a sledovateľné poplatky a mikropoplatky.

6 Funkčné požiadavky na služby M2M

6.1 Zber a hlásenie dát

Systém M2M musí podporovať hlásenie zo špecifického zariadenia M2M alebo sieťového priechodu M2M alebo skupiny zariadení M2M alebo skupiny sieťových priechodov M2M spôsobom požadovaným aplikáciou M2M nasledovne:

- periodické hlásenie s časovou periódou definovanou aplikáciou M2M;
- hlásenie na požiadanie s dvomi možnými režimami. Jeden je okamžitý zber a hlásenie dát, ďalší je hlásenie dát, ktoré boli vopred zaznamenané v označenom špecifickom časovom intervale;
- plánované hlásenie;
- hlásenie udalostí.

6.2 Diaľková kontrola zariadení M2M

Systém M2M musí podporovať schopnosť aplikácie diaľkovo kontrolovať zariadenia M2M, ktoré podporujú túto vlastnosť.

6.3 Skupiny

Systém M2M musí podporovať mechanizmus na vytvorenie a zrušenie skupín a začleniť jednotku do skupiny, modifikovať obmeny (napríklad charakteristiky) členov skupiny, odstrániť jednotku zo skupiny, vypísať členov skupiny, kontrolovať členstvo jednotky v skupine, vyhľadať jednotky v skupine a identifikovať všetky skupiny kde jednotka je členom.

6.4 Kvalita služby (QoS)

Systém M2M musí využívať kvalitu služby (QoS) podporovanú základnými sieťami. Aplikácie alebo vlastnosti služby M2M môžu použiť vlastnosti QoS základných sietí, ak sú v systéme realizované.

6.5 Výber typov zariadení/sieťových priechodov

Systém M2M musí podporovať množstvo rozličných typov zariadení/sieťových priechodov M2M, napríklad aktívnych zariadení M2M a zariadení M2M v pohotovostnom stave, aktualizovaných zariadení/sieťových priechodov M2M a neaktualizovaných zariadení/sieťových priechodov M2M.

Systém M2M musí podporovať činnosti viazané na parameter kde parametrom sú kontrolovateľné prostriedky CPU, veľkosť pamäte, úroveň batérie a pod.

6.6 Príjem informácie

Systém M2M musí podporovať nasledovný mechanizmus na prijímanie informácií zo zariadení M2M a sieťových priechodov M2M:

- prijímanie nežiadaných informácií (pasívne získavanie);
- prijímanie plánovaných informácií;

- prevádzkovanie osobitných algoritmov na vyberanie informácií (napríklad algoritmus „round robin“, náhodne v danom časovom okne, algoritmus „round robin“ pre skupiny s náhodným opakovaním v danom časovom okne).

6.7 Prístupnosť

Systém M2M môže mať informácie o stave prístupnosti objektov.

6.8 Asymetrické toky

Zariadenia a sieťové priechody M2M musia podporovať asymetrické toky.

6.9 Rozmanitosť trás

Systém M2M musí podporovať výberový príjem fyzických trás, ak to požaduje aplikácia M2M.

6.10 Heterogénne miestne siete M2M

Systém M2M musí umožniť prepojenia heterogénnych miestnych sietí M2M. To sa môže dosiahnuť v sieťovom priechode M2M.

6.11 Zber a doručovanie informácií na viacnásobné aplikácie

Systém M2M musí podporovať schopnosť vo viacnásobných aplikáciách M2M spolupracovať s rovnakými zariadeniami súčasne.

6.12 Manažérstvo viacerých zariadení/sieťových priechodov M2M

Aplikácia M2M musí spolupracovať s jedným alebo viacerými zariadeniami/sieťovými priechodmi M2M, napríklad na zber informácií, kontrolu, priamo alebo použitím vlastností služby M2M.

6.13 Opis zariadení/sieťových priechodov M2M

Charakteristiky M2M zariadenia/sieťového priechodu M2M môžu sa jednak vopred konfigurovať v systéme M2M alebo poskytovať zariadením/sieťovým priechodom M2M k systému M2M. Charakteristiky poskytované zariadením/sieťovým priechodom M2M majú prioritu oproti vopred konfigurovaným charakteristikám.

Charakteristiky M2M obsahujú statickú informáciu sú vlastnosti M2M, ktoré sa môžu priradiť k zariadeniam a sieťovým priechodom M2M a dynamické informácie – lokalita, stav, dostupnosť, ktoré sa môžu priradiť k zariadeniam a sieťovým priechodom M2M.

7 Bezpečnosť

V tejto kapitole sú spracované požiadavky na bezpečnosť systému M2M. Doplnené sú základné požiadavky dôvernosti, integrity, overovania totožnosti a oprávnenia a uvedené sú špecifické príklady možných napadnutí, pred ktorými sa systém musí chrániť.

7.1 Overovanie totožnosti

Systém M2M musí podporovať vzájomné overovanie totožnosti riadiaceho systému M2M a zariadenia M2M alebo sieťového priechodu, a jednocestné overovanie totožnosti zariadenia M2M alebo sieťového priechodu chrbticou M2M. napríklad vzájomné overovanie totožnosti sa môže požadovať medzi poskytovateľom služby a jednotkou požadujúcou službu. Strany môžu zvoliť stupeň overenia totožnosti na umožnenie primeranej úrovne bezpečnosti.

Každá služba musí sa vykonávať nezávisle na iných službách.

Zariadenia M2M spojené cez sieťový priechod M2M: overovanie totožnosti zariadenia M2M sa môže vykonávať priamo k systému M2M alebo k overenému sieťovému priechodu M2M.

7.2 Vlastnosti vrstvy overenia totožnosti služby M2M alebo aplikácií M2M

Ak existuje požiadavka na prístup dát alebo prístup zariadenia/sieťového priechodu M2M, zariadenie M2M alebo sieťový priechod M2M musí vzájomne overovať totožnosť s vlastnosťami služby M2M alebo aplikáciami M2M, od ktorých je prijatá požiadavka prístupu.

7.3 Dôvernosť dátového prenosu

Systém M2M musí podporovať príslušnú dôvernosť výmeny dát. Osobitne aplikácia M2M môže alebo nepožaduje použitie takej dôvernosti.

7.4 Integrita dát

Systém M2M musí podporovať overovanie integrity vymieňaných dát.

7.5 Ochrana pred zneužitím pripojenia siete

Riešenie bezpečnosti M2M musí chrániť pred neoprávneným použitím zariadenia/sieťového priechodu M2M.

7.6 Súkromie

Systém M2M musí chrániť súkromie.

7.7 Viacnásobní používatelia

Viacnásobní používatelia sú obsiahnutí v službe M2M medzi koncovými bodmi. Systém M2M musí umožniť takým rozdielnym používateľom doručiť službu v spolupráci, udržiavanie bezpečnosti služby medzi koncovými bodmi.

Napríklad služby M2M môžu zahŕňať troch rozličných účastníkov prispievajúcich k doručeniu služby. Prevádzkovateľ bunkovej siete môže byť oddelený od poskytovateľa aplikácie M2M. Tretia strana, ktorá môže byť zahrnutá je prevádzkovateľ M2M alebo prevádzkovateľ virtuálnej mobilnej

siete (MVNO), ktorý sa nachádza medzi prevádzkovateľom bunkovej siete a poskytovateľom aplikácie. Ak MVNO je zahrnutý typicky zohráva úlohu prevádzkovateľa siete domáca sieť bunkového zariadenia M2M je s MVNO, napríklad MVNO má vstup HLR/HSS na zariadenie.

7.8 Overovanie integrity zariadenia/sieťového priechodu

Systém M2M musí podporovať mechanizmus na overovanie integrity zariadenia/sieťového priechodu M2M. Zariadenie/sieťový priechod M2M môže alebo nesmie podporovať overovanie integrity. Ak zariadenie/sieťový priechod M2M podporuje overovanie integrity a ak overovanie zariadenia/sieťového priechodu zlyhá zariadenie/sieťový priechod nesmie umožniť vykonať overovanie totožnosti zariadenia/sieťového priechodu.

Mechanizmus overenia integrity zariadenie/sieťový priechod sa môže aktivovať po dopyte zo systému M2M alebo sa môže samostatne štartovať miestne zariadením/sieťovým priechodom M2M vždy.

Systém M2M môže diaľkovo získať historický záznam detekcie narušenia v zariadení/sieťovom priechode, ak je podporovaný zariadením/sieťovým priechodom.

7.9 Dôveryhodné a bezpečné prostredie

Zariadenia M2M, ktoré požadujú overovanie integrity zariadenia musia poskytovať dôveryhodné vykonávacie prostredie. Doveryhodné prostredie (TrE) musí tvoriť logická jednotka, ktorá poskytuje dôveryhodné prostredie na výkon citlivých funkcií a ukladanie citlivých dát. Všetky dáta produkované cez vykonávanie funkcií v TrE nesmú byť identifikovateľné neoprávnenými vonkajšími jednotkami. TrE musí vykonávať citlivé funkcie (ukladanie dôverných kľúčov a poskytovanie kryptografických výpočtov používajúcich tieto dôverné kľúče) potrebné na vykonávanie kontroly integrity zariadenia M2M a overovanie zariadenia.

7.10 Bezpečnostný kredit a aktualizácia softvéru na aplikačnej úrovni

Ak je dovolené bezpečnostnou politikou, systém M2M musí mať funkcionalitu diaľkovo poskytovať nasledujúce funkcie, na aplikačnej úrovni:

- bezpečná aktualizácia softvéru a firmvéru cez zariadenie/sieťový priechod M2M na bezpečnosť aplikácie;
- bezpečná aktualizácia kontextu (dôverné kľúče a algoritmus) cez zariadenie/sieťový priechod M2M na bezpečnosť aplikácie.

Funkcia sa musí poskytovať v prostredí odolnom proti prieniku, napríklad TrE alebo bezpečnostný prvok v zariadeniach/sieťových priechodoch M2M podporujúci túto funkciu.

8 Identifikátory, číslovanie a adresovanie

8.1 Identifikátory

Systém M2M musí dosahovať zariadenia M2M alebo sieťové priechody M2M pomocou jednotlivých identifikátorov zariadení M2M alebo identifikátorov sieťového priechodu M2M.

Systém M2M musí byť pružný v podpore viac ako jedného identifikačného systému.

8.2 Identifikácia

Systém M2M musí podporovať identifikáciu CO alebo skupiny CO podľa ich identifikátorov, dočasného identifikátora, pseudonymu (napríklad rozličné identifikátory do rovnakej jednotky), lokality alebo ich kombinácie (napríklad, URI alebo IMSI).

Musí sa umožniť opakované využívanie identifikátorov určitej kategórie zariadení alebo zariadení pracujúcich v určitých prostrediach (napríklad, viazaný prostriedok).

8.3 Adresovanie

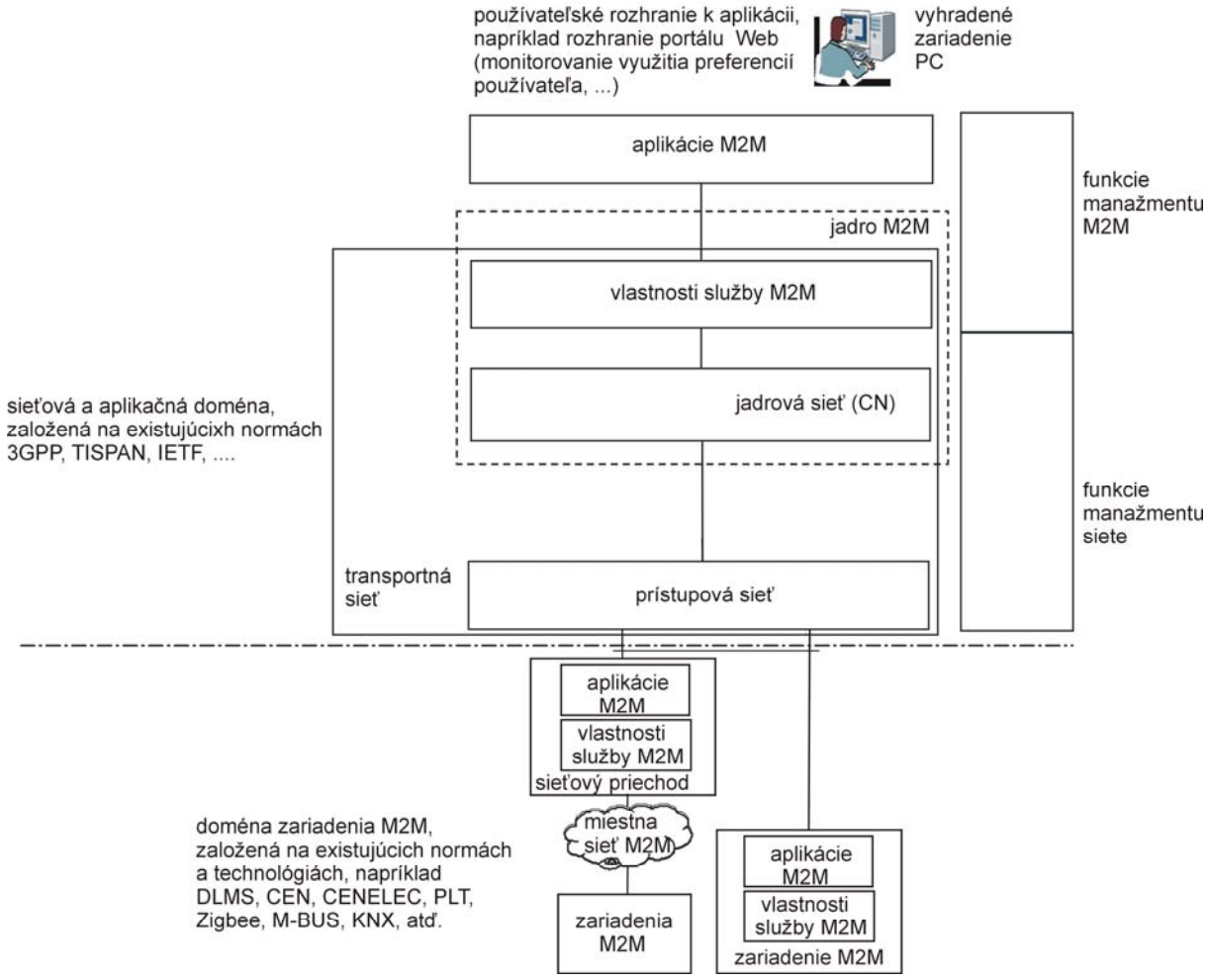
Systém M2M musí umožniť pružné systémy adresovania, vrátane:

- adresy IP – CO;
- skupinových adries IP – CO (vrátane adresy skupinového vysielania);
- adries E.164 – CO (napríklad, MSISDN).

Príloha A (informatívna) – Prehľad systému M2M

A.1 Architektúra hornej úrovne systému

Na umožnenie pochopenia určitých výrazov použitých v tomto dokumente, obrázok A.1 znázorňuje architektúru hornej úrovne systému M2M (HLSA).



Obrázok A.1 – Prehľad hornej úrovne systému M2M

Architektúra M2M obsahuje doménu zariadenia M2M a domény siete a aplikácií. HLSA je založená na existujúcich normách ohľadne sieťovej domény rozšírenej o špecifiká M2M.

Príloha B (informatívna) – Prípady použitia M2M

B.1 Prípady použitia M2M zovšeobecnené z SCP UICC

Nasledujúce prípady použitia sú zovšeobecnené z [i.8] UICC v aplikáciách stroj-stroj (M2M).

B.1.1 Prípady použitia sledovania a vyhľadávania

Prípady použitia sledovania a vyhľadávania sa týkajú hlavne automobilizmu, ale sa týkajú aj sledovania a vyhľadávania tovarov vo výrobe a maloobchode, napríklad založené na technológii RFID.

Aplikácie M2M v automobilovom priemysle sú zamerané na doručenie zdokonalenej bezpečnosti pre ľudí (aplikácie tiesňových volaní) alebo aktív (aplikácie sledovania odcudzenia). Aplikácie riadenia vozidiel zamerané na zvýšenie účinnosti prevádzkovania a zvýšenie prírastkových výnosov. Tieto služby sú v širokom rozsahu a obsahujú diaľkovú diagnostiku, navigačné systémy, mýtne poplatky (poistenie, služby vo vozidle), a pod.

V prípadoch použitia v automobilovom odvetví sú spoločné automobilové kritériá. Výbor pre automobilovú elektroniku (AEC) bol založený na vytvorenie spoločných noriem na kvalifikáciu súčiastok a systému kvality na priame určovanie spoľahlivosti výrobku. Technická komisia pre súčiastky v AEC je normalizačný orgán na vytvorenie noriem pre spoľahlivé, vysokokvalitné elektronické súčiastky.

Automobilový trh vo zvýšenej miere požaduje, že dodávatelia polovodičov poskytujú výrobky zhodné s normami AEC-Q100 a ISO 16750 [i.7] (poskytuje pravidlá týkajúce sa podmienok prostredia spoločne elektrických a elektronických systémoch inštalovaných v automobiloch) do zariadení M2M a modulov, ktoré musia spĺňať všetky tieto požiadavky.

Prípad použitia – tiesňové volanie

Systém tiesňového volania vo vozidle môže zachrániť životy automaticky alebo manuálne vyslaním presnej polohy a informácie vodiča k tiesňovému stredisku. V tomto prípade použitia, komunikačný modul M2M vo vozidle umožňuje prenos údajov tiesňového volania medzi vozidlom a službou tiesňových volaní.

V tomto prípade použitia, vozidlo má vstavaný komunikačný modul M2M, ktorý je pripojený k snímačom, ktoré môžu určiť vznikajúcu nehodu. V prípade nehody modul automaticky zriadi spojenie k tiesňovému stredisku a vyšle informáciu o lokalite, indikáciu o stupni nehody a možno iné dodatočné informácie, ktoré môžu byť prístupné a vyhodnotené užitočné (tieto služby sa môžu realizovať aplikáciami umiestnenými v module M2M). Hlavné kritérium v tomto prípade použitia je, že modul M2M a jeho rozhrania sú schopné vydržať a pracovať po náraze spôsobenom nehodou. Ďalej, automobilový priemysel naznačuje že veľkosť modulu M2M a schopnosť modulu komunikovať v normálnom automobilovom prostredí počas predpokladanej životnosti vozidla, sú dôležité.

Prípad použitia – Manažérstvo vozidla

V tomto prípade použitia, vozidlo má vstavaný komunikačný modul M2M, ktorý je zvyčajne vlastnený spoločnosťou (nie používateľom). Modul zbiera informácie napríklad, lokalitu, časy, nával prevádzky, údržbové údaje a podmienky prostredia dopravy. Tieto informácie sa môžu vyslať modulom cez mobilnú sieť k aplikačnému serveru, kde sa môžu použiť na sledovanie vozidla a tovaru.

Využívaním vyhľadanej informácie, aplikačný server môže účinne optimalizovať plán a trasu doručovania. Nastavený plán doručenia je potom vyslaný cez mobilnú sieť k vozidlu a príslušná

informácia sa môže zobraziť pre vodiča. Ďalej informácie týkajúce sa údržby, údržba sa môže plánovať alebo sa môže vykonávať diaľková údržba. Ďalej snímače prostredia sa môžu použiť na vyhľadanie informácie o prostredí skladovania tovaru a podmienkach dopravy výrobku.

Hlavné kritérium v tomto prípade použitia je schopnosť komunikačného modulu M2M komunikovať pokiaľ je v normálnom automobilovom prostredí počas predpokladanej životnosti vozidla.

Prípad použitia – sledovanie odcudzených áut

V súčasnosti, odcudzenie automobilov je obyčajne chránené jedným z dvoch spôsobov, jednak odstrašením zlodeja poplachovým systémom alebo zabránením naštartovania motora imobilizérom. Tieto systémy sa predsa len môžu prekonať, napríklad rýchlou deaktiváciou alebo ignorovaním poplachového systému alebo prepravou vozidla bez pomoci motora.

V tomto prípade použitia, zavedenie M2M umožní zamedzenie samotného odcudzenia alebo zachytenia vozidla, napríklad sledovaním odcudzenia. Uvažuje sa, že modul M2M umožní bezpečnú komunikáciu v sieti s jednotkou tretej strany.

M2M v tomto prípade použitia bude fungovať v rozšírenom rozsahu teploty a vlhkosti nie bežných v koncových zariadeniach. Ďalej spojenie s komunikačným modulom bude odolávať vibráciám produkovaných motorom vozidla aj vozidlom na ceste. Ochrániť modul M2M od útrap rovnakého osudu početné poplachové systémy, je nutné zabezpečiť proti krádeži a chybnému použitiu, napríklad cez M2M UICC k vozidlu a alebo párovaním komunikačného modulu.

Iným činiteľom v tomto prostredí je často obmedzený priestor, dostupný na ukrytie alebo zabezpečenie systému proti krádeži a chybnému použitiu, čo znamená že veľkosť modulov M2M musí byť malá na to, aby boli dostupné pre veľký segment automobilového trhu v niektorých prípadoch, modul M2M musí byť integrovaný s masovo vyrábanými modulmi to všeobecne požadujú skupiny automobilových výrobcov. Ak sú vozidlá navrhnuté na životnosť, ktorá sa môže jednoducho rozšíriť na viac ako 10 rokov, ale tiež udržiavať minimálne náklady na údržbu, predpokladaná životnosť je tiež činiteľ.

B.1.2 Monitorovanie prípadov použitia

Aplikácie M2M v tejto kategórii sú použité na monitorovanie a kontrolné spotrebiteľské služby, alebo monitorovanie, sledovanie a vyhľadávanie osôb, zvierat alebo majetku.

Prípad použitia – služby spojené s meraním/zálohovou platbou (voda, plyn, elektrina)

Služby spoločností využívajúcich inteligentné meracie služby inštaláciou komunikačných modulov M2M na merané zariadenia, ktoré môžu vyslať informáciu automaticky alebo na požiadanie k aplikačnému serveru, ktorá sa môže napríklad použiť na automatické účtovanie meraného prostriedku, v tomto prípade použitia účelom je jednak zlepšiť energetickú výkonnosť a účinnosť cez doručenie oveľa viac presnejšieho obrazu o spotrebe, účinnosti a nákladoch, ako aj tiež doručenie aktuálneho využitia bez ľudského sprostredkovania. To tiež nastaví poskytovanie kladného vplyvu na prostredie. V opačnom smere informácia v meracom zariadení sa môže bezpečne aktualizovať (vzduchovým komunikačným rozhraním).

Meracie zariadenia sú často umiestnené v nešetrných prostrediach. V mnohých meracích zariadeniach je tiež veľmi obmedzený priestor, znamená to, že veľkosť komunikačného modulu M2M je potrebné minimalizovať. Meracie zariadenia sa môžu vyrábať vo veľkých objemoch, ktoré požadujú, že moduly M2M sa môžu integrovať v priemyselných procesoch. Citlivé údaje sa môžu uložiť, moduly je potrebné chrániť pred krádežou a chybným použitím.

Rozšírenie uvedeného prípadu použitia na meranie plynu, elektriny, vody je založené na zálohových platbách. Domácnosť si môže predplatiť zakúpenie špecifického množstva plynu, elektriny, vody apod. Informácia o zakúpenom množstve je bezpečne prenesená (vzduchovým komunikačným rozhraním) k meraciemu zariadeniu a potom bezpečne uložená v moduloch M2M.

Počas spotreby aktuálna informácia o spotrebovanom množstve sa prenesie k modulu M2M. Ak zakúpené množstvo bolo spotrebované dodávka sa môže ukončiť.

Tento prípad použitia znamená schopnosť vykonávať bezpečné transakcie medzi modulom M2M a kontrolovaným meracím zariadením. To tiež môže obsahovať možnosť bezpečne vykonávaných kontrolných činností, napríklad ukončenie dodávania.

Prípad použitia – ochrana osoby/zvieraťa

V tomto prípade použitia osoby a alebo zvieratá sú vybavené prenosným zariadením obsahujúcim komunikačný modul M2M a voliteľne funkciou GPS, ktorá vysiela informáciu automaticky alebo na požiadanie k aplikačnému serveru, ktorý môže monitorovať stav a umiestnenie osôb alebo zvierat. Účelom je zlepšiť bezpečnosť a alebo diaľkovo monitorovať stav pokiaľ je tiež schopné sledovať a vyhľadávať osobu alebo zviera. Tieto služby sa môžu realizovať aplikáciami umiestnenými v module M2M/UICC.

Pre osoby, typické aplikácie sú osamelý pracovník, zdravotná starostlivosť, monitorovanie prestárlych alebo detí. Pre zvieratá, typická aplikácia je sledovanie a vyhľadávanie.

Prenosné zariadenia sú často umiestnené v namáhaných prostrediach; to znamená, že sú podrobené silným vibráciám alebo pravidelným nárazom. Priestor je veľmi obmedzený, znamená to, že veľkosť komunikačného modulu M2M má byť minimálna. Aby sa mohli uložiť citlivé údaje, modul sa potrebuje chrániť proti krádeži a chybnému použitiu.

Prípad použitia – Ochrana objektu

Tento prípad použitia je veľmi podobný predchádzajúcemu (ochrana osôb/zvierat). Objekty sú vybavené prenosnými zariadeniami obsahujúcimi komunikačný modul M2M a voliteľne funkciu GPS, ktorá vysiela informáciu automaticky alebo na požiadanie k aplikačnému serveru, ktorý môže monitorovať stav a umiestnenie týchto objektov. (Tieto služby sa môžu realizovať aplikáciami umiestnenými v module M2M/UICC).

Účelom tejto aplikácie je sledovanie a vyhľadávanie.

Prenosné zariadenia sú často umiestnené v nevľúdnych prostrediach. To znamená, že sú vystavené silným vibráciám alebo pravidelnému nárazu, extrémnej teplote, vlhkosti alebo ničivým prostrediam ako je slaná voda.

Priestor je tiež veľmi obmedzený, znamená to, že veľkosť komunikačného modulu M2M je nutné minimalizovať. V mnohých prípadoch zariadenie musí byť dostatočne malé, aby sa mohlo ukryť.

Aby sa mohli uložiť citlivé údaje, modul je potrebné chrániť proti krádeži a chybnému použitiu.

B.1.3 Prípady použitia na transakcie

Prípad použitia – terminály PoS (platobné terminály)

V súčasnosti platobné terminály sú pripojené cez pevné spojenia. Na použitie v miestach ako sú bary, reštaurácie apod. To znamená, že sú montované alebo umiestnené v pevnej pozícii a osoba, ktorá chce vykonať transakciu potrebuje ísť na miesto platobného terminálu. To spôsobuje ťažkosti pre predávajúceho/čašníka ako aj pre zákazníka. V prípade vzdialených platobných terminálov, napríklad parkovacích automatov, automatov predaja cestovných lístkov apod. Tieto požadujú pevné spojenie, ktoré je často ťažké a nákladné inštalovať a môže byť tiež vystavené poškodeniam. Iná možnosť je pripojiť platobné terminály cez (miestne) rádiové spojenie, ktoré zavádza určité bezpečnostné obmedzenia.

Zavedenie modulov M2M do tohto prostredia umožňuje dodatočné možnosti v aplikáciách, ako sa môžu inštalovať komunikačné moduly M2M do rádiových platobných terminálov, pouličných

parkovacích automatov a automatov predaja cestovných lístkov, napríklad na poskytovanie komunikácií na transakcie s kreditnými alebo debetnými kartami s priamym prístupom. Použitie komunikačného modulu M2M môže poskytovať bezpečný komunikačný kanál.

Obyčajne tieto zariadenia obsahujúce komunikačný modul budú potrebovať splniť špecifické požiadavky na bezpečnosť finančných transakcií.

B.1.4 Prípady použitia na kontrolu

Prípad použitia – kontrola predajných automatov

V súčasnosti predajné automaty sú umiestnené v rozličných lokalitách ako, napríklad vo vnútri úradov, verejných budov, verejných priestranstiev, železničných staníc apod. Opakované plnenie a údržba predajných automatov v súčasnosti daná vyhradeným personálom, ktorý navštevuje predajné automaty v pravidelných intervaloch na kontrolu úrovní náplne, opakované plnenie automatov, vykonávanie údržby a identifikácie poškodení alebo funkčných porúch.

Začlenenie M2M do tohto prostredia umožní dodatočné možnosti optimalizácie činnosti predajných automatov. Umožnením prístupu k (mobilnej) telekomunikačnej sieti moduly M2M sa môžu použiť na vstavanie komunikačných modulov M2M na poskytovanie overených informácií o aktuálnom stave predajného automatu cez sieť k službe na pozadí. Cez toto spojenie je možné prenášať informácie o aktuálnych úrovniach naplnenia, stave údržby, možných poškodeniach, funkčných poruchách apod. Dodatočne je možné prenášať aktualizáciu napríklad cenových informácií alebo vykonávania diaľkovej údržby. Týmto spôsobom predajné automaty je nutné navštíviť len na základe požiadavky.

Prípad použitia – kontrola výrobných strojov

V súčasnosti výrobné stroje sú umiestnené normálne vo výrobných priestoroch, ktoré v závislosti na týchto priestoroch môžu vystaviť výrobný stroj nevľúdnym prostrediam. Oprava a údržba výrobných strojov je v súčasnosti vykonávaná vyhradeným personálom, ktorý navštevuje výrobné stroje v pravidelných intervaloch na opravu, vykonanie údržby a identifikácie poškodení alebo funkčných porúch.

Začlenenie M2M do tohto prostredia umožní dodatočné možnosti na optimalizáciu činnosti výrobných strojov. Umožnením prístupu k mobilnej telekomunikačnej sieti moduly M2M sa môžu použiť na vstavanie komunikačných modulov M2M na poskytovanie overených informácií o aktuálnom stave predajného automatu cez sieť k službe na pozadí. Cez toto spojenie je možné prenášať informácie o aktuálnych úrovniach naplnenia, stave údržby, možných poškodeniach, ktoré vedú k funkčným poruchám apod. Dodatočne je možné prenášať aktualizáciu, napríklad aktualizovaný softvér alebo vykonávať diaľkovú údržbu, napríklad cez funkciu vzdušného komunikačného rozhrania. Týmto spôsobom predajné automaty je nutné navštíviť len na základe požiadavky.

B.2 Prípady použitia na odmenu za prácu

B.2.1 Služby spojené s manažmentom účtovania zálohovej platby

Zákazník s predplateným programom, prijíma indikáciu (napríklad cez miestny displej), že jeho predplatené konto je už vyčerpané. Teda aktivuje opakované naplnenie konta, napríklad cez miestny displej, aplikáciu home-banking alebo mobilným telefónom. Príslušný mechanizmus používa dôvernú tretiu stranu (napríklad bankovú spoločnosť alebo spoločnosť s kreditnou kartou) na overovanie a vykonanie opakovaného plnenia konta.

B.2.2 Poplatok za odčítanie snímačov

Poskytovateľ služby ponúka odčítanie snímačov teploty vody v atraktívnych oblastiach pri mori na kúpanie spoplatnené 1/50 Euro za každé odčítanie. Schéma odmeny za prácu požaduje počítačové mikro platby určené s nastavením cenovej efektívnosti.

B.2.3 Ďalšie oblasti použitia

- v doprave/logistike kde, napríklad vodič môže registrovať doručenie tovaru a prijať platbu;
- aplikácie EPOS;
- platby NFC, napríklad cez MS.

Všetky tieto oblasti majú prospech z vlastností elektronickej odmeny za prácu.

B.2.4 Vlastnosti a primitívy služby

Vyúčtovanie a kompenzácia je časťou domény manažmentu. Nasledujúce primitívy vyššej úrovne sa môžu použiť na vyúčtovanie akéhokoľvek páru objektov (napríklad kompenzátor a kompenzovaný). Predbežná podmienka na vyúčtovanie je, že objekt má platné konto a reláciu s vzájomne dôveryhodným sprostredkovateľom (napríklad bankou):

- CommitValue – odovzdaná hodnota (objektová identifikácia predávajúceho Object-ID Vendor, mena kurz Currency currency, príkaz na vytvorenie Integer Devidedby, objektová identifikácia sprostredkovateľa Object-ID Broker);
- Settle – zaplatiť (objektová identifikácia predávajúceho Object-ID Vendor, príkaz na vytvorenie suma Integer Amount, objektová identifikácia sprostredkovateľa Object-ID Broker).

B.2.5 Príklad schémy poplatkov

Kandidát kompenzačnej schémy realizujúci uvedené primitívy služby sa môže zakladať na nasledovnej mikrokompenzačnej schéme. Významné výhody mikrokompenzácie v makrokompenzácii je pružnosť umožňujúca akúkoľvek diskrétnosť hodnoty v transakcii.

Objekt generujúci hašovací reťazec z dĺžkou N používajúci hašovaciu funkciu N krát k náhodnej dôvernej hodnote PN, vykoná odmocninu hašovacieho reťazca na získanie konečnej hašovacej hodnoty P0, znaku hašovacieho reťazca. Objekt odovzdá reťazcu digitálnym podpisom znak s privátnym kľúčom. Za každú platbu, objekt uvoľní predbežné zobrazenie poslednej hašovacej hodnoty. Napríklad objekt uvoľní hašovaciu hodnotu P1 na prvú platbu. Prijímač platby môže použiť rovnakú hašovaciu funkciu s hodnotou P1 na získanie znaku P0. Pretože hašovacia funkcia

je jednocestná, len objekt môže generovať hašovaciu hodnotu. Objekt odovzdá znak k reťazcu P0, dĺžku reťazca, hodnotu na každú hašovaciu funkciu a obchodníka od ktorého si praje spotrebovať reťazec. Pred platením objekt smeruje povinnosť k obchodníkovi, ktorý môže overiť svoju pôvodnosť (napríklad offline). Na každú mikroplatbu objekt uvoľní nasledovné (množstvo) platobných hašovacích funkcií v reťazci. Obchodník môže odkúpiť späť hašovaciu funkciu u sprostredkovateľa, pri ktorom objekt má konto neskoršieho dátumu, prezentujúce hašovaciu funkciu najvyššieho platenia spolu s platnou zmluvou. (existuje optimalizácia tejto schémy).

Nasledovné primitívy služby realizujú schopnosť dĺžky počtu znamienok (vrátené v značkách), každá hodnotená a honorovaná obchodníkom (napríklad cez makrotransakciu):

- nákupné značky (Buy-Tokens) (objektová identifikácia sprostredkovateľa Object-ID Broker, dĺžku príkazu Integer Length, hodnotu príkazu Integer Value, objektová identifikácia predávajúceho, Object-ID Vendor, hašovacia hodnota P0 Hash P0).

Značka odovzdanej hodnoty Commit-Token sa používa na inicializáciu kompenzácie a umožní obchodníkovi overiť platnosť znamienok cez sprostredkovateľa:

- značka odovzdanej hodnoty Commit-Token (objektová identifikácia predávajúceho Object-ID Vendor, objektová identifikácia sprostredkovateľa Object-ID Broker, dĺžka príkazu Integer Length, hodnota príkazu Integer Value, hašovacia hodnota P0 Hash P0).

Explicitná mikrokompanzácia je vytvorená vyvolaním primitívy:

- vystavené značky Submit-Tokens (objektová identifikácia predávajúceho Object-ID Vendor, dĺžka príkazu Integer Length, hašovacia značka Hash Tokens).

Dĺžka počtu znamienok je prenášaná obchodníkom.

Funkcia vystavených znamienok Submit-Tokens sa môže integrovať v iných primitívach, napríklad v primitívach prenášaných správ.

Obchodník používa na spätné odkúpenie značiek nasledovných primitív (napríklad miktoplatby):

- spätné odkúpenie značky Redeem–Token (objektová identifikácia sprostredkovateľa Object-ID Broker, hašovacia značka Hash Tokens).

B.3 Príklady použitia automatizácie domácnosti

Komunikácia M2M môže zohrať hlavnú úlohu v domácnostiach, kde automatizácia určitých procesov sa ukázala dôležitá v mnohých častiach domácnosti ako je pohodlie, zdravie, bezpečnosť, energetická účinnosť apod.

Rozvoj automatizácie domácnosti obsahuje požiadavky služby, ktoré sa môžu odvodiť z opisu určitých priradených prípadov použitia, ako je uvedené nasledovne.

B.3.1 Energetická účinnosť domácnosti

Účelom prípadu použitia je použitie komunikácie M2M na optimalizáciu použitia energie v domácnosti. Napríklad, niektoré snímače obyvateľov budú použité na získanie informácie o tom či je niekto alebo nikto v miestnosti. V prípade, ak nikto, svietidlá sa automaticky vypnú. Tento základný príklad sa môže rozšíriť na iné typy snímačov v rozličných miestnostiach domácnosti na kontrolu spotreby energie z rozličných zariadení. Snímače a akčné jednotky sú pripojené jednak rádiom alebo vodičmi (napríklad, cez PLC) k sieťovému priechodu M2M. Zbieranie údajov z rozličných snímačov (napríklad meranie spotreby elektriny kúrenia, detekcie prítomnosti, snímače vonkajšej teploty), sieťový priechod M2M môže vyslať príslušné povely (napríklad vypnúť kúrenie v miestnosti alebo v celej domácnosti) k akčným jednotkám v závislosti na kontexte miestnej informácie (napríklad nikto nie je v domácnosti počas určitého obdobia). Systém M2M teda umožní redukovať spotrebu energie automatickým prispôsobením použitia zariadení v domácnosti k miestnym parametrom.

V prípade použitia, zaradenie heterogénnych technológií použitých snímačov a akčných jednotiek sa vykonáva v sieťovom priechode M2M, ktorý spracúva všetky prijaté údaje, zatrieďuje ich k iným súvisiacim informáciám a vysiela príslušné povely k akčným jednotkám na základe spracovania.

Pri snímačoch a akčných jednotkách, ktoré sa využívajú v domácnostiach sa predpokladá použitie nízkovýkonových spotrebných technológií (špeciálne tých snímačov a akčných jednotiek použitých na účely energetickej účinnosti) tak, že koncový používateľ nepotrebuje dlhodobo nahradiť ich batérie. To je tiež potrebné s praktických príčin, ak snímače alebo akčné jednotky sú inštalované na niektorých miestach s ťažkým prístupom.

Prípad použitia tiež súvisí s monitorovaním energie, informovaním zákazníka o jeho spotrebe energie, globálne alebo podrobne (zariadenie od zariadenia), s možným diaľkovým prístupom, aby bol informovaný o tejto spotrebe, aj keď koncový používateľ nie je doma. Môže tiež upozorniť používateľa na akúkoľvek detegovanú nepravidelnosť v porovnaní s bežnou spotrebou, tak, že akýkoľvek únik nemôže nastať v príslušnom čase.

Príloha C (informatívna) – Bezpečnostné hľadiská

C.1 Dôveryhodné a bezpečné prostredie

Určité zariadenia M2M obyčajne pracujú bez obsluhy a nechránené ľuďmi a teda sú predmetom zvýšených úrovní bezpečnostných ohrození, ako sú fyzické manipulovanie, napadnutie, neoprávnené monitorovanie apod. Koncové zariadenia môžu byť tiež geograficky rozptýlené po čase. Takéto zariadenia M2M musia teda poskytovať primeranú bezpečnosť na detegovanie a na bránenie sa útokom. Zariadenia môžu tiež potrebovať podporovať diaľkový manažment vrátane aktualizácie firmvéru na opravu porúch alebo obnovu po zlomyseľných útokoch.

Pri určitých zariadeniach M2M sa obyčajne požaduje, aby boli malé, lacné, schopné pracovať bez ľudskej obsluhy vo zvýšených časových intervaloch a komunikovať cez rádiové miestne siete (WAN) alebo WLAN. Zariadenia M2M sa obyčajne využívajú v prevádzke už mnoho rokov a po rozmiestnení, smerujú k požadovaniu funkcií diaľkového manažmentu. Je pravdepodobné, že zariadenia M2M sa budú rozširovať vo veľmi veľkých množstvách a mnoho z nich bude tiež mobilných, vytvárajúcich nereálne alebo nemožné pre prevádzkovateľov alebo zákazníkov vyslať personál na ich kontrolu alebo servis. Tieto požiadavky zavádzajú množstvo unikátnych bezpečnostných algoritmov do zariadení M2M, ktoré komunikujú v rádiových komunikačných sieťach.

Pracovná skupina bezpečnosti (SA3) projektu partnerstva tretej generácie (3GPP) zhromaždila kategórie ohrozenia:

1.) Fyzické útoky vrátane vloženia platnej značky overenia totožnosti do zmanipulovaného zariadenia, vkladanie a alebo zavedenia podvodného alebo upraveného softvéru (reflashing), a environmentálnych útokov/na strane kanála, obidva pred a po využívaní v prevádzke.

2.) Útoky na konfiguráciu ako sú podvodná aktualizácia softvéru/zmeny konfigurácie; chybná konfigurácia vlastníkom, účastníkom alebo používateľom; a chybná konfigurácia alebo odhalenie zoznamov na kontrolu prístupu.

3.) Protokolové útoky priamo proti zariadeniu, ktoré obsahuje útoky “človek v strede” po prvom prístupe k sieti. Útoky na vyradenie služby (DoS), odhalenie zariadenia využívaním slabých stránok aktívnych sieťových služieb a útokov cez manažment vzduchového rozhrania (OAM) a jej prevádzky.

4.) Útoky na chrbticovú sieť hlavné ohrozenie prevádzkovateľa mobilných sietí (MNO), vrátane falošnej prezentácie zariadení; tunelovanie prevádzky stroj-stroj bez obsluhy; chybná konfigurácia firevalu v modeme, smerovači alebo sieťových priechodoch; útoky DoS proti chrbticovej sieti; tiež zmena oprávnenej fyzickej lokality zariadenia neoprávneným spôsobom alebo útoky na sieť pomocou podvodného zariadenia.

5.) Útoky na používateľské dáta a identitu súkromia vrátane odpočúvania dát používateľa alebo dát zariadenia vyslaných v prístupovej sieti; maskovanie iného zariadenia používateľa/účastníka; odhalenie sieťovej identifikácie používateľa alebo iných dôverných dát pre neoprávnené strany.

Nasledujú určité odkazy na požiadavky na bezpečnosť vyplývajúce z diskusií pri spracovaní špecifikácií M2M:

- Podľa dokumentu funkčnej architektúry M2M (TS 102 690 [i.1]), zariadenia M2M poskytujú bezpečný prenos správ. Funkcie citlivé na bezpečnosť sa musia vykonávať v bezpečnom prostredí. Tiež na zaistenie že správa je bezpečná, vykonávacie programy poskytujú bezpečnosť šifrovania a na prenos správ sa musí kontrolovať integrita pred uvedením do

prevádzky. Kontrola integrity sa vykonáva v bezpečnom vykonávacom prostredí ktoré odoláva zlomyseľným útokom a neoprávnenému prístupu.

- Zariadenia musia podporovať presnú a bezpečnú časovú synchronizáciu. Na zabezpečenie, že synchronizačný softvér je bezpečný, softvér musí vykonať program v bezpečnom prostredí a musí sa kontrolovať integrita a overovanie pred jeho vykonávaním.

- Zariadenie M2M musí podporovať bezpečnú a sledovateľnú kompenzáciu a mikrokompenzáciu. Na zaistenie, že softvér/firmvér potrebný na generovanie informácie o kompenzácii a kryptografické kľúče potrebné na overovanie totožnosti a kompenzáciu sú overené a bezpečné z hľadiska integrity. Kontrola integrity firmvéru sa musí vykonávať v bezpečnom a dôvernom prostredí v zariadení M2M. Bezpečné prostredie musí poskytovať bezpečné úložisko potrebných kľúčov a dát. Také bezpečné úložisko nemá byť dostupné neoprávneným používateľom.

- V prípade použitia M2M na inteligentné merania TR [i.2], poskytovateľ inteligentného merania môže aktivovať alebo zariadenie M2M má schopnosť hlásiť stav bezpečnosti zariadenia. Tento monitorovací a vykazovací softvér musí byť bezpečný proti zlomyseľným modifikáciám a teda pracovať v bezpečnom prostredí.

Ďalej aplikácia zariadení M2M, ktorá generuje merania alebo informácie, ktoré sú počitateľné a zúčtovateľné alebo zariadenia M2M, ktoré požadujú overovanie integrity zariadenia, musia poskytovať dôveryhodné bezpečné vykonávacie prostredie alebo dôveryhodnú platformu na vykonávanie aplikácií, ktoré požadujú zabezpečené vykonávacie prostredie. Teda predpokladá sa, že tieto zariadenia M2M poskytujú dôveryhodné a bezpečné vykonávacie prostredie. TrE má poskytovať bezpečné úložisko a odolávať zlomyseľným a neoprávneným prístupom. Majú mať tiež kontrolovanú integritu a byť overený pred začatím alebo vykonávaním činnosti dôverným hardvérom.

TrE môže byť logicky oddelená jednotka v M2ME, obsahujúca všetky nevyhnutné prostriedky na poskytovanie dôveryhodného prostredia na prevádzku softvéru a ukladanie citlivých dát. Od TrE sa očakáva poskytovanie izolácie softvéru a uložených dát ich oddelením od zvyšku M2ME, teda chrániť ich pred neoprávneným prístupom. Od TrE sa očakáva poskytovať bezpečný verejný kľúč, ktorý bude zabezpečený proti vniknutiu meraniami bezpečnosti hardvéru. Osobitne sa očakáva poskytovanie základnej dôvernosti (RoT) na bezpečnú činnosť. Od RoT sa očakáva, že bude nemennou časťou TrE, ktorá bude zabezpečovať vnútornú činnosť a bude schopná charakterizovať schopnosti alebo identitu systému k vonkajším jednotkám. Na základe RoT, TrE sa má vykonať bezpečný proces spustenia umožňujúci, že TRE dosiahne zistený dôveryhodný stav.

Napríklad, TrE môže byť zostavený z neodstrániteľného a nemenného hardvéru založeného na podstate dôvernosti spôsobom bezpečného procesu zavedenia procesu. Bezpečný proces zavedenia má obsahovať kontroly, vykonávané RoT, integrity každého zavedeného alebo počiatočného prvku zariadenia M2M a bude tiež obsahovať kontroly vykonávané TrE po štarte každého zavedeného alebo štartovacieho prvku zariadenia M2M, iného ako RoT alebo TrE. TrE môže uložiť najmenej jeden kryptografický kľúč, ktorý je fyzicky viazaný na zariadenie M2M. TrE môže použiť taký kľúč na overovanie totožnosti TrE k systému M2M a tiež chrániť dôvernosť a integritu komunikačných správ do zariadenia kontrolujúceho integritu a overovanie medzi zariadením M2M a systémom M2M.

Príloha D (informatívna) – Výklad textov s ohľadom na určité požiadavky

Počas návrhu tohto dokumentu, sa navrhli príspevky na požiadavky s výkladom textov oprávňujúcich potrebu týchto požiadaviek. Po úprave textu V 0.3.1 tohto dokumentu bolo rozhodnuté vymazať všetky výklady textov s cieľom mať požiadavky textov jednoznačne znázornené. Už niektoré výklady textov môžu pomôcť lepšiemu pochopeniu počiatočnej súvislosti, podľa ktorej bola navrhnutá požiadavka. Teda boli nakopírované do tejto informatívnej prílohy.

D.1 Výklad textov určitých požiadaviek článku 4

D.1.1 Súvisiacich s článkom 4.1

Aplikácia M2M v sieťovej a aplikačnej doméne musí mať funkciu aktivácie komunikácie so zariadením M2M aj keď je použité dynamické adresovanie na sieťovej vrstve.

Niektoré aplikácie M2M môžu požadovať komunikáciu partner-partner medzi objektmi, napríklad medzi sieťovým priechodom a aktivátorom na miestne spracovanie, napríklad v kontexte automatizácie domácnosti. Teda, komunikačné toky medzi týmito objektmi sa musia podporovať.

D.1.2 Súvisiacich s článkom 4.2

Zariadenia M2M s batériou môžu mať dlhý pohotovostný čas.

Aplikácie M2M musia vysielať správu ku zariadeniam M2M v pohotovostnom stave, napríklad, a mať ju doručenú k zariadeniu sieťou, ak zariadenie sa prihlási. Aplikácia nemusí byť zaťažená s ponechaním sledovania ak zariadenie sa prihlási, špeciálne do zariadenia za sieťovým priechodom, napríklad za koordinátorom Zigbee.

D.1.3 Súvisiacich s článkom 4.3

Určité aplikácie M2M v sieti a aplikačnej doméne požadujú aby boli doručené rovnaké správy k množstvu zariadení M2M. Doručenie sa môže realizovať kombináciou individuálneho a skupinového vysielania v závislosti na typoch prístupovej siete.

D.1.4 Súvisiacich s článkom 4.4

V mnohých aplikáciách M2M je všeobecná pružnosť v ktorej dáta sú zbierané zo zariadenia M2M alebo zasielané do zariadenia M2M. Napríklad, v inteligentnom meraní môže byť dostatočné odčítanie merača jedenkrát za hodinu, a ktoré bude v akomkoľvek čase v každej hodine. Systém M2M bude mať prospech zo schopnosti plánovať dátový prenos, ak sieť je najmenej nepriechodná ako to zníži náklady na komunikáciu.

D.1.5 Súvisiacich s článkom 4.5

V určitých aplikáciách M2M zariadenie M2M môže obsahovať funkcionalitu komunikácie v technológiách s viacnásobným prístupom ako sú pevné a rádiové s rozličnými komunikačnými nákladmi v čase. Aplikácie M2M budú mať prospech z výberu primeranej trasy.

D.1.6 Súvisiacich s článkom 4.6

Aplikácie M2M musia komunikovať so zariadeniami za jednotkou translátora sieťových adries (NAT). Napríklad, v prípade sietí snímačov v domácnosti snímače a koordinátor snímača sú za sieťovým priechodom domácnosti.

D.1.7 Súvisiacich s článkom 4.7

Niekedy správa, že aplikácia chce sieť na doručenie nemôže byť doručená v špecifikovanom časovom intervale, pretože napríklad určitý uzol siete je v poruche. V takých prípadoch aplikácie M2M v sieti a aplikačných doménach musia prijať potvrdenie o komunikačných poruchách.

D.1.8 Súvisiacich s článkom 4.8

Systém M2M sa musí navrhnúť na dosiahnutie pružnosti a minimalizovania vzhľadom na využitie prostriedku systému. Počet snímacích uzlov, kontrolérov a akčných členov (napríklad objektov) napríklad vyžívaných v mestskom prostredí na podporu určitých aplikácií sa predpokladá že bude veľmi vysoký (napríklad v rozsahu od 10^2 do 10^7).

D.1.9 Súvisiacich s článkom 4.13

Nie všetky aplikácie M2M môžu mať vplyv na integritu prenášanej informácie. Inak povedané, integrita informácie doručená so službami M2M môže byť veľmi dôležitá v iných aplikáciách M2M.

D.1.10 Súvisiacich s článkom 4.15

Určité aplikácie M2M môžu požadovať rovnakú službu M2M na spoľahlivejšom a trvalom základe. V tomto prípade bude dobré, ak sieť môže vytvoriť trvalé spojenie, ktoré bude trvalé aj po čase, ak je individuálny prenos informácie úplný. Toto trvalé spojenie by sa mohlo zakázať, ak prostriedok siete, ktorý ho požaduje tak koná alebo dokiaľ neuplynie časovač. Inak povedané, aplikácie M2M môžu použiť služby M2M veľmi zriedka a nepravidelne bez akejkoľvek možnosti predpovedať ako skoro po prvej požiadavke sa služba M2M môže znovu požadovať. V tomto prípade, sieť bude potrebovať poznať, že spojenie sa môže zrušiť po individuálnej požiadavke, ak je prenos informácie úplný.

D.1.11 Súvisiacich s článkom 4.20

Komunikácia M2M ako je generovanie informácie vyššej hodnoty použitej na spoplatnenie môže požadovať časovú pečiatku. Pri takejto komunikácii je potrebné generovať bezpečnú a dôvernú časovú pečiatku, ktorá sa môže použiť v sieti a zariadení.

D.2 Výklad textov s ohľadom na určité požiadavky článku 5

D.2.1 Súvisiacich s článkom 5.1.3

Skúšanie spojenia smerom k určitým CO (podľa zmluvy so zákazníkom) v pravidelných intervaloch je v požiadavke viac aplikačných oblastí. Skúšku môže aktivovať aplikácia alebo CO a udalosti kde spojenie nie je overené sú zaznamenané a hlásené.

D.2.2 Súvisiacich s článkom 5.1.5

Zariadenia M2M môžu byť v prevádzke funkčné mnoho rokov. Určité zariadenia môžu pracovať v oblastiach kde je ťažký fyzický prístup k zariadeniu. Napríklad snímače M2M montované v náročných prostrediach alebo zariadenia M2M na geografické vyhľadávanie. Takéto zariadenia sa ťažko obsluhujú ľudským zásahom. Aj keď zariadenia M2M sú projektované na veľkú životnosť, ak zariadenie M2M zaznamená poruchu, potom diaľkový manažment takýchto zariadení poskytuje pre uvedenú službu výmenu zariadenia. Takéto poruchy sa môžu vyvolať napríklad náročným prostredím, poruchou systému a prelomením bezpečnosti. Navrhuje sa, že zariadenia M2M môžu podporovať diaľkový manažment alebo premiestnenie zariadenia. V takom riadiacom procese, zariadenie môže mať funkcionalitu aktualizácie firmvéru bezpečným pripojením k manažovaciemu

serveru. Po aktualizácii firmvéru, aplikácie, zariadenia sa môžu opakovane uviesť do známeho a konzistentného stavu.

D.2.3 Súvisiacich s článkom 5.2.1

Služby M2M obyčajne obsahujú veľký počet zariadení M2M, ale každá všeobecne vysiela malé množstvo dát. Výnosy na zariadenie M2M sú všeobecne malé pre každého zákazníka v hodnotovom reťazci. Dôležité je zníženie výdavkov vynaložených pri využívaní a údržbe týchto zariadení. Jeden hlavný krok vo využívaní zariadení M2M je ich zriaďovanie vo vhodnej dátovej základni siete a poskytovateľa aplikácie. Osobitne, zriaďovanie kľúčov alebo iných informácií o riešenie bezpečnosti musí byť jednoduché a modulárne. Proces zriaďovania nepredpokladá, že zariadenie M2M bude zapnuté v známom vopred navrhnutom špecifickom čase. Zariadenia sa môžu zapnúť dočasne zo strany výrobcu na skúšanie, ale potom sa následne vypne až do využívania. Môžu sa inštalovať v jednom čase, ale potom komunikácia môže byť zriadená neskôr. Nie je možné predpovedať osobitný čas na vykonanie procesu zriadenia.

D.2.4 Súvisiacich s článkom 5.2.2

Sieť musí mať funkcionalitu obnovenia spojenia, ak objekt vypadol a na miesto sa vložil nový objekt. Nové objekty sa môžu tiež inštalovať práve na zvýšenie spoľahlivosti a výkonnosti siete. Zmena sa musí lokalizovať a musí byť neviditeľná pre všetkých v sieti. Časový interval na opravy siete môže byť relatívne dlhý, ako vo fáze zavádzania.

D.2.5 Súvisiacich s článkom 5.2.3

Na vykonávanie presných meraní na multiplovaných zariadeniach M2M v podrobných rovnakých prípadoch v čase, časová synchronizácia s presnosťou ms je možno potrebná, vo veľkej fyzickej oblasti. Objekty v pohotovostnom stave môžu požadovať potrebu rovnako vyššej synchronizácie na udržanie účinného občasného spojenia.

D.2.6 Súvisiacich s článkom 5.2.4

Manažment, napríklad zariadenia na strane zákazníka (CPE), prevádzkové zariadenia vrátane prvkov domény zariadenia M2M a objektov je kľúč k ponúkaniu služby a prevádzkovej účinnosti.

D.3 Výklad textov s určitými požiadavkami článku 6

D.3.1 Súvisiacich s článkom 6.1

V závislosti na aplikácii M2M, zber dát sa môže realizovať rozdielnymi spôsobmi. Napríklad informácia z požiarneho hlásiča sa musí doručiť akonáhle je detegovaná, ale spotreba energie v domácnosti sa požaduje len niekedy. Systém M2M musí podporovať rozličné spôsoby doručenia dát v čase.

D.3.2 Súvisiacich s článkom 6.3

Hlavný prvok návrhu je skupina. To je konštrukcia architektúry, ktorá sa môže použiť pre veľký rozsah a rozsiahle distribučné siete a ponúka spôsob základného vytvárania skupín a segmentácie. Takýto mechanizmus umožňuje použiť zložitejšiu funkcionalitu a riadenie neriešiteľných problémov v aktuálnych sieťach. Princípom je, že sa virtualizuje každý horizontálny segment v súčasnej internetovej štruktúre odhalenej tesne spojenej federácie samostatne definovaných, pracujúcich a riadených jednotiek. Pokladá sa za prirodzené uvažovať každú z týchto existujúcich jednotiek v skupine siete, každá skupina má koherentnú vnútornú technológiu a politiky, a každá skupina si riadi svoje interakcie s inými skupinami siete podľa určitých

definovaných súborov pravidiel a politík. Skupina je jednotka, ktorá zapúzdruje a realizuje pôsobenie, skupinovanie, rozdeľovanie a prekračovanie hraníc súborov jednotiek. V sieťových systémoch sú použité tieto funkcie na množstvo účelov, vrátane riadenia odstupňovania, heterogenity, bezpečnosti, spoplatnenia, výkonnosti, dôvernosti apod. Je znázornené, že máme zvláštny mechanizmus na účel, poskytovaním jedného vysoko optimalizovaného a opakovateľne použiteľného generického mechanizmu na obsluhu množstva účelov.

D.3.3 Súvisiacich s článkom 6.4

V kritických aplikáciách je povinná podpora QoS. Nasledovné parametre služby sú dôležité v sieti s vynútenými prostriedkami, nie je to konečný zoznam:

- šírka pásma – šírka pásma sa môže prideliť špecifickému toku trvalo alebo v časovom intervale; niektoré toky môžu tiež spoločne využívať šírku pásma negarantovaným spôsobom;
- oneskorenie – čas na výber dát pri prechode sieťou od zdroja k cieľu; môže sa vyjadrovať výrazom: konečný termín doručenia;
- prenosová fáza – prevádzka aplikácií sa môže synchronizovať koordinovanými prenosmi;
- prednosť a zrušenie priority – siete môžu mať obmedzené prostriedky, ktoré sa môžu meniť v čase; to znamená systém sa môže stať úplne predplatený alebo temer predplatený; systémové politiky určia ako sú pridelené prostriedky, ak prostriedky sú predplatené; možnosti sú blokovanie a vybraná degradácia;
- prenosová priorita – spôsoby, ktorými sú pridelené medzi viacnásobné služby obmedzené prostriedky v objektoch; na prenos objekt má vybrať, ktorý paket v jeho zásobníku sa vyšle v ďalšej prenosovej možnosti; priorita paketu je použitá ako jedno kritérium na výber ďalšieho paketu; na príjem objekt má rozhodnúť ako uloží prijatý paket; objekty sú obyčajne pamäťovo závislé a prijímacie zásobníky môžu byť plné; priorita paketov sa použije na výber, ktoré pakety sa uložia alebo vyradia;
- spoľahlivosť – dáta poskytované na ďalšie spracovanie sa musia prenášať spoľahlivo, ak sa stratí jedna časť celého dátového súboru, úplná vzorka dát môže byť neužitočná;
- vlastnosti trasy – schéma obnovy trasy môže byť rozličná v závislosti na funkcii trasy v poruche.

D.3.4 Súvisiacich s článkom 6.5

Sieť musí podporovať rozličné typy objektov, napríklad aktívne objekty a objekty v pohotovostnom stave. Tiež určité zariadenia obsahujú malé objekty s nízkou výkonnosťou, malými kapacitami pamäte, procesormi s nízkym výkonom, nízkou šírkou pásma, vysokou stratovosťou apod. Požiadavky na funkcie zariadení M2M musia byť vhodné s ohľadom na obmedzené hardvérové konfigurácie.

Spracovanie objektov v pohotovostnom stave je kritickou požiadavkou, pretože objekty môžu zostať v pohotovostnom režime po väčšinu času. Časová synchronizácia je dôležitá na účinné smerovanie paketov. Spojenie musí byť spoľahlivé napriek nereagujúcim objektom následkom periodickej hybernácie.

Sieť musí podporovať činnosti s vynúteným parametrom, kde parameter sú kontrolovateľné prostriedky ako CPU, veľkosť pamäte, úroveň batérie apod.

Systém M2M musí šetriť spotrebu napájania nenapájaných zariadení M2M. Napájané objekty musia pomáhať nenapájaným objektom alebo starať sa o viac funkcií ako nenapájané objekty.

D.3.5 Súvisiacich s článkom 6.7

Následkom externých faktorov alebo programovaných rozpojení, objekt môže byť v niekoľkých stavoch spojenia, v rozsahu od “vždy spojený” k “zriedka spojený”.

D.3.6 Súvisiacich s článkom 6.8

Dátové toky medzi objektmi nie sú nevyhnutne symetrické. Osobitne asymetrické náklady a jednocestné trasy sú spoločné pri prezentovaní dát a poplachoch, ktoré predstavujú významnú časť prevádzky zariadenia M2M. Hlásenie dát odčítaných veľkým množstvom priestorovo rozptýlených uzlov smerom k niekoľkým sieťovým priechodom bude viesť k vysoko smerovaným informačným tokom. Sťahovanie (napríklad nových funkcií) k objektom jednoducho spôsobí asymetriu v smere k objektu.

D.3.7 Súvisiacich s článkom 6.9

Kategórie rozličných služieb majú meniace sa požiadavky na službu a často nie je želateľné mať rozličné trasy v rozličných dátových tokoch, hoci medzi rovnakými dvomi koncovými bodmi. Napríklad poplachové alebo periodické dáta z A do Z môžu požadovať rozmanitú trasu so špecifickým oneskorením a spoľahlivosťou. Prenos súboru medzi A a Z nesmie mať rozmanitú trasu, ale vysokú dátovú rýchlosť.

D.3.8 Súvisiacich s článkom 6.10

Architektúra systému M2M musí podporovať spojenie existujúcich a vyvíjaných prístupových technológií pevných a rádiových, vrátane domácich sietí s nízkym výkonom rádiových komunikácií s krátkym rozsahom. Prepojenie rozmanitých technológií môže požadovať funkciu sieťového priechodu, ktorú môžu poskytovať prevádzkovatelia siete.

D.3.9 Súvisiacich s článkom 6.11

V niektorých prípadoch, určité rozdielne aplikácie M2M môžu použiť rovnaké zariadenia M2M. Prípad použitia tohto variantu: ak nastane prevádzková nehoda, poškodené vozidlo hlási informáciu k službe zdravotného strediska a poisťovacej spoločnosti. Systém M2M musí mať funkcionalitu podpory prenosu dát zo zariadení M2M k jednému alebo viacerým aplikáciám.

D.3.10 Súvisiacich s článkom 6.12

Obyčajne aplikácia M2M obsluhuje viac ako jedno zariadenie M2M na poskytovanie služieb M2M k zákazníkom. Príklady obsahujú inteligentné dopravné systémy a inteligentné meracie systémy obidva podporujú veľký počet zariadení M2M.

D.4 Výklad textov s ohľadom na určité požiadavky článku 7

D.4.1 Súvisiacich s článkom 7.1

Server priebehu procesov, ktorý zbiera dáta zo zariadenia M2M musí mať spätnú informáciu, že dáta prichádzajú z oprávneného a správneho zariadenia. Ak neexistuje takéto overovanie totožnosti, určité zariadenia môžu predstierať iné zariadenia v sieti a vysielať dáta. Napríklad v inteligentnej meracej službe kde merané dáta sa zbierajú z rozličných meračov, podvodný vlastník domácnosti ich môže zmeniť k serveru tak, že sa to javí ako susedov merač, teda zabráni plateniu za používanie elektriny.

Postup overenia totožnosti môže tiež pomôcť eliminovať chyby z nedbalosti, ako je rovnaká identita nastavená na viacnásobné zariadenia, v prípade, ak identita snímača sa nastavuje dvojpolohovými prepínačmi.

D.4.2 Súvisiacich s článkom 7.2

Zariadenia môžu byť napadnuté narušiteľom v závislosti od charakteru dát, ktoré poskytujú alebo pre ich vlastnosti pôsobenia, robia si nárok stať sa aplikačným serverom priebehu procesov. Variant kde takýto útok má určitú ekonomickú hodnotu pre narušiteľa je diaľková kontrola domácich automatizovaných zariadení, ako sú poplachové zariadenia alebo automatický vrátnik garážových dverí. Predstieraním funkcie sieťového automatizovaného servera v domácnosti, narušiteľ môže deaktivovať poplach a otvárač dverí na vstup do domácnosti. Teda zariadenie musí overiť totožnosť servera pred akceptovaním akýchkoľvek dát, takých ako sú príkazy alebo aktualizácia manažmentu.

D.4.3 Súvisiacich s článkom 7.3

V mnohých aplikáciách M2M dáta zbierané zo zariadení M2M majú dôverný charakter. Napríklad v aplikáciách sledovania dieťaťa nie je možné pre neoprávnené osoby získať informáciu o lokalite dieťaťa. Riešenie bezpečnosti M2M musí byť také, aby nebolo možné získať informáciu o deťoch získavanú odpočúvaním v akomkoľvek bode siete.

D.4.4 Súvisiacich s článkom 7.4

Narušitelia majú výhodu z modifikácie dát prenášaných zo zariadenia k aplikačnému serveru priebehu procesov alebo viac menej cez útoky “človek v strede”. Musí sa umožniť overenie integrity dát prenášaných medzi jednotkami.

D.4.5 Súvisiacich s článkom 7.5

Na rozdiel od prípadu spotrebných elektronických zariadení zákazníka, v mnohých prípadoch zariadenia M2M sú vlastnené poskytovateľmi aplikácie a využívané v priestoroch, ktoré nie sú trvalo fyzicky monitorované alebo chránené. Napríklad v prípade inteligentného merania, merače typicky vlastnia obslužné spoločnosti a využívajú sa v domácnostiach a malých podnikateľských lokalitách. Tieto zariadenia sú teda chúlostivejšie na odcudzenie. Nesprávne použitie ukradnutých komunikačných modulov nájdených v týchto zariadeniach na účely normálnej internetovej komunikácie ako je internetové prehľadávanie sa nesmie povoliť.

D.4.6 Súvisiacich s článkom 7.6

V mnohých aplikáciách sa neakceptuje prenos aktuálnej nekryptovanej identity zariadenia, pretože zariadenie alebo jeho využitie môže sledovať narušiteľ odpočúvaním siete. Identita sa dá hodnotiť a môže sa korelovať s inými dátami ako lokalizácia sieťových prvkov, z ktorých sa nadobudne informácia o identite na rozlíšenie určitých charakteristík.

D.4.7 Súvisiacich s článkom 7.8

Zariadenia M2M budú obyčajne využívané v prevádzke nestráženej a nemonitorovanej ľuďmi alebo inými prostriedkami. Mnoho zariadení M2M bude tiež spracovávať pridanú hodnotu, spoľahlivé dáta pri aplikáciách, ktoré majú dôsledky na bezpečnosť v príslušnom trhovom sektore M2M (napríklad inteligentné meranie, senzorové siete, kamery na dopravnú prevádzku, zariadenia ITS apod.). Mnoho takýchto zariadení sa môže realizovať platformami s otvorenými rozhraniami v prípadoch ako je zníženie nákladov, zlepšenie funkcionality a pružnosti a jednoduchý vývoj. Všetky uvedené faktory znamenajú, že prelomenie HW, FW alebo SW zariadení M2M predstavuje reálne bezpečnostné znepokojenie. Útočník, napríklad môže byť schopný použiť trhliny v sieti a zlé

sieťové priechody alebo ešte rozhrania na zariadení na vloženie malvéru alebo iných napadnutí zariadenia M2M, spôsobiacich zničenie alebo poškodenie záujmových osôb. Ohrozenie je špeciálne záležitosťou zariadení M2M, ktoré sa môžu pripojiť samostatne k internetu cez verejné komunikačné siete.

D.4.8 Súvisiacich s článkom 7.10

Očakáva sa, že do určitej doby vzrastie množstvo služieb M2M a varianty prípadu použitia. Ďalej určité služby M2M môžu mať dlhé produktové cykly a dlhú životnosť, napríklad inteligentné merače. Experti na bezpečnosť a kryptografiu často objavujú nové útoky na systémy. Sú spojené s trvalými zlepšeniami vlastností počítačov, a často nútia manažérov s hľadiska bezpečnosti aktualizovať dĺžky kľúča a modifikovať bezpečnostnú politiku. V niektorých prípadoch si situácia môže vyžadovať aktualizáciu algoritmu. V niektorých iných prípadoch sa môže vyžadovať distribúcia bezpečnostnej opravy na určenie ohrozenia v protokoloch a aplikáciách, ktoré neboli známe počas inštalácie. Všeobecnejšie, prevádzkovatelia ako aj poskytovatelia aplikácie M2M môžu objaviť v časovom intervale nové potreby na aktualizáciu služby a bezpečnostných politík.

História

História dokumentu		
V1.1.1	August 2010	Publikovanie