PRIMENA NAJSAVREMENIJIH TEHNOLOGIJA ZAŠTITE PODATAKA U DISTRIBUIRANIM AMR SISTEMIMA

M. STEFANOVIĆ, E-Smart Systems, Beograd, Srbija
V. PEJOVIĆ, E-Smart Systems, Beograd, Srbija
V. BAJIĆ, E-Smart Systems, Beograd, Srbija
M. KOJIĆ VELjOVIĆ, E-Smart Systems, Beograd, Srbija

UVOD

Uvođenjenjem AMR (*Automated Meter* Reading) rešenja u svoje poslovne procese, elektrodistribucija ostvaruje jedan od prvih koraka ka dostizanju ciljeva 20-20-20 postavljenih od strane Evropske Komisije (1). Prvi i osnovni benefiti koji se postižu jesu smanjenje netehničkih gubitaka, povećanje tačnosti merenja i generalno unapređenje postojećih poslovnih procesa. Sa druge strane, sigurnost podataka jeste osnovni preduslov za ispravan rad kompletnog sistema.

U distribuiranom AMR sistemu, postoji nekoliko nivoa na kojima se osetljivi podaci čuvaju i obrađuju. Pre svega, to su napredna brojila, koja se nalaze kod krajnjih korisnika i koja, prema tehničkim zahtevima EPS-a (2), čuvaju odgovarajuće podatke neko vreme u svojim arhivama. Na ovom nivou je onemogućeno neautorizovano čitanje ili izmena ovih podataka poštovanjem predviđenih standarda (3) koji definišu nekoliko nivoa pristupa za čitanje ili parametrizaciju brojila. Sa druge strane, informaciona infrastruktura u elektrodistribucijama, već ima razrađene mehanizme zaštite podataka. Ono što ostaje kao problem jeste zaštita linka od brojila do informacionog centra. Ovaj link može biti direktan, u slučaju kada se očitavanje izršava preko GPRS komunikacionog kanala direktno iz centra, ili sa nekoliko među tačaka – Koncentrator podataka, Komunikacioni server, AMR Centar, MDM (*Meter Data Management*) Centar. U oba slučaja potrebno je obezbediti poverljivost, integritet i dostupnost informacija koje prolaze zadatim linkom.

U ovom radu ćemo prikazati mehanizme i tehnologije koje su korišćene za zaštitu podataka u projektu SESAME-S (sesame-s.ftw.at) gde je bilo potrebno preneti podatke od Koncentratora podataka do baze podataka smeštene u AMR Centru, a zatim deo prikupljenih podataka publikovati autorizovanim licima i servisima na Cloud platformi.

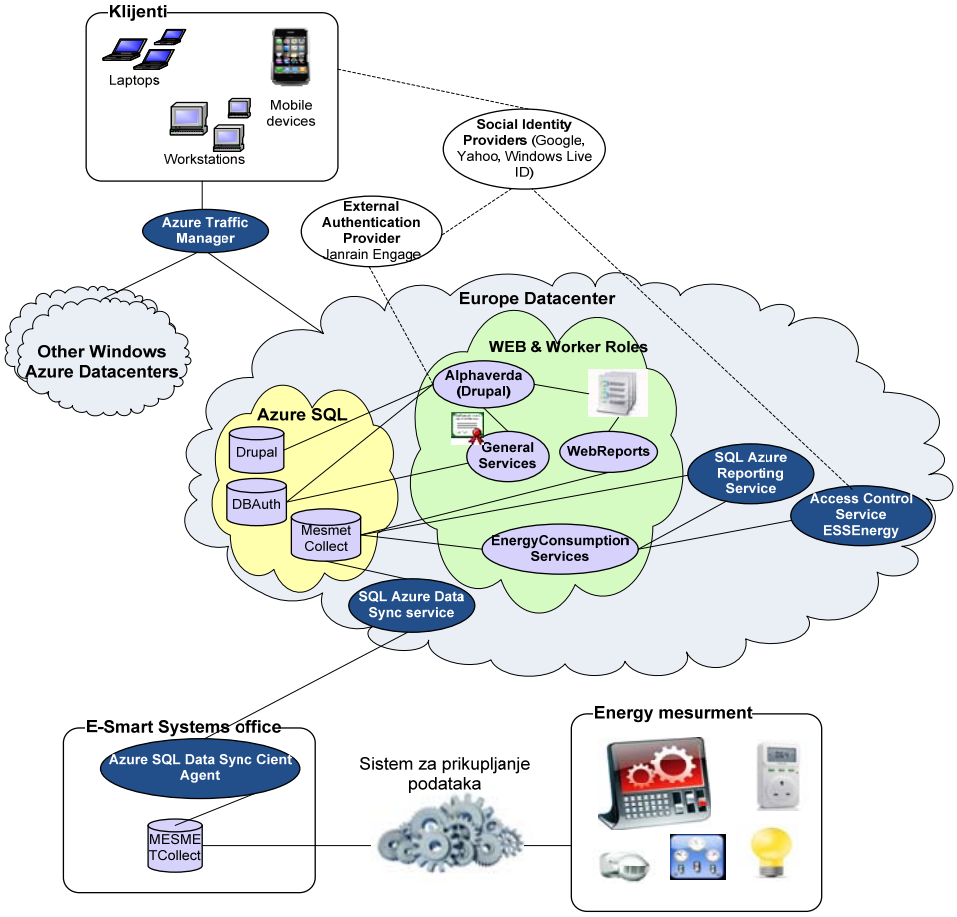
OPIS SISTEMA

Pomenuti projekat se bavi prikupljanjem podataka o korisnicima, njihovim parametrima potrošnje, podataka o vremenskoj prognozi, aktuelnim tarifnim profilima, planiranim akcijama elektrodistributera i ostale informacije koje bi svim učesnicima u sistemu mogle da pruže korisne servise. Svi podaci se čuvaju u okviru Cloud platforme, gde se obrađuju i odakle se preko posebnog Web portala prezentuju zainteresovanim i autorizovanim korisnicima. Cloud platforma (4) obezbeđuje operativni sistem, infrastrukturne i aplikativne servise za hostovanje razvojnih aplikacija i servisa. Za potrebe projekta SESAME-S izabrana je Micosoft Windws Azure platforma kao Cloud platfoma.

Kao jedan od izvora podataka, instalirana su napredna brojila kod krajnjeg korisnka. Na ovom mestu je instaliran i računar sa Windows 7 operativnim sistemom i sa skupom Windows Servisa koji su putem odgovarajućeg hardverskog adaptera i PLC mreže očitavali brojila u zgradi, izvršavali osnovnu obradu podataka i sinhronizovali podatke preko Interneta u bazu AMR Centra. Za potrebe sigurnog prenosa podataka do AMR Centra razvijen je mehanizam baziran na elementima simetrične i asimetrične kriptografije.

U delu prenosa podataka od AMR Centra do Cloud okruženja koje je podignuto na Microsoft Azure platformi iskorišćen je jedan od postojećih mehanizama zaštite podataka koji je obezbeđen preko Microsoft Azure SQL Data Sync servisa o kome će kasnije biti reči.

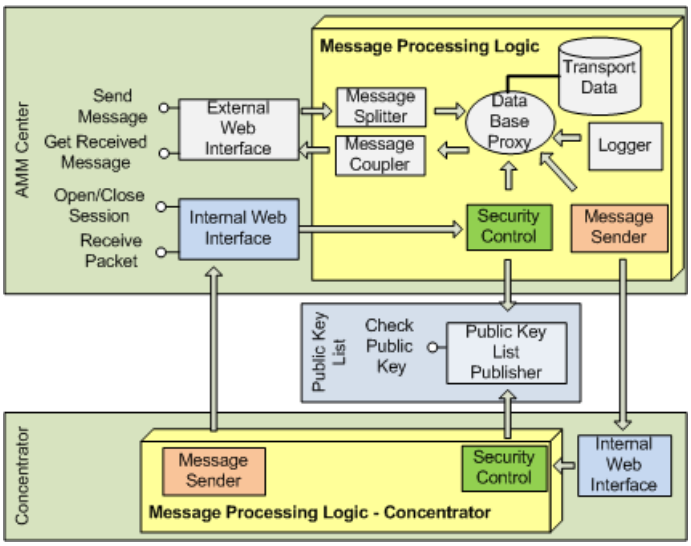
Naredna slika prikazuje osnovne kanale komunikacije između komponenti sistema SESAME-S. Svi kanali komunikacije koji prenose osetljive podatke su zaštićeni korišćenjem SSL-a.



Slika 1 – Zaštita podataka i kanala komunkacije SESAME-S aplikacija i servisa

Zaštita podataka u prenosu do AMR Centra

Za potrebe sigurnog prenosa podataka od računara kod Korisnika do baze u AMR Centru korišćen je transportni servis prikazan na Slici 2. Servisi na računaru kod korisnika (Concentrator) i na strani AMR Centra koriste jedini interfejs prema ovom modulu – *External Web Interface*. Poruke se između dva modula prenose preko Web servisa *Internal Web Interface*. Paketizacija, kompresija i enkripcija poruka za slanje, kao i sklapanje, dekompresija i dekripcija primljenih paketa se izvršava u komponentama *Message Processing Logic* celine. Prilikom uspostavljanja sesije, vrši se obostrana provera identiteta. Istorija uspostavljanja sesija se beleži u lokalnoj bazi podataka *Transport Data*.



Slika 2 – Schema rada transportnog modula

Simetričnom kriptografijom se enkriptuje sadržaj poruka koje se prenose, dok se asimetrična kriptografija koristi za enkripciju simetričnog ključa i za mehanizam potvrde identiteta učesnika u komunikaciji. Dužina RSA ključeva je 2048 bita. Autorizovano telo se nalazi na lokaciji AMR Centra i na sigurnom mestu čuva tri para Master RSA ključeva (*M1pub/M1priv, M2pub/M2priv, M3pub/M3priv*) kojima će se potpisivati javni RSA ključevi, jedinstveni po svakom učesniku u komunikaciji. Ovi potpisi se koriste za potvrdu pripadnosti familiji učesnika u komunikaciji.

Prilikom instalacije transpotnog modula na strani korisnika, izvršava se sledeće:

- Generišu dva para RSA ključeva
  - *Epub* i *Epriv* – par ključeva za enkripciju simetričnog ključa
  - *Spub i Spriv* – par ključeva za potvrdu identiteta
- Upisuju javni ključevi *M1pub*, *M2pub* i *M3pub*
- Upisuju potpisi javnih ključeva *Spub* i *Epub* privatnim ključevima *M1priv*, *M2priv* i *M3priv*
  - *M1Sign(Epub)*, *M2Sign(Epub)*, *M3Sign(Epub)*
  - *M1Sign(Spub)*, *M2Sign(Spub)*, *M3Sign(Spub)*

Svi ključevi i potpisi se čuvaju na Smart kartici koja ide uz računar koji se daje korisniku.

Odmah po generisanju, javni ključevi Spub i Epub kao i njihovi potpisi se zavode u listi komponente Public Key List čiji je interfejs Public Key List Publisher dostupan svim učesnicima u komunikaciji.

Komunikaciju može da inicira bilo koja strana koja želi da pošalje poruku tako što pozivom metode *SendMessage()* na *External Web Interface* servisa predaje sadržaj poruke i adresu odredišta (adresa *Internal Web Interface* servisa na odredištu). Izračunava se Hash poruke koji se, zajedno sa novogenerisanim simetričnim ključem *SymKey,* enkriptuje sa *Epriv* ključem, a poruka se kompresuje, enkriptuje *SymKey* ključem i na kraju paketizuje. Ove informacije se čuvaju u lokalnoj bazi odakle se komponentom *Message Sender* izvršava slanje poruke na odredište.

Prvi korak u slanju poruke jeste uspostavljanje sesije sa odredištem. Komponenta *Message Sender* poziva metodu *OpenSession* na *Internal Web Interface* servisu odredišta i pri tome prosleđuje odgovarajuće ključeve i potpise. U slučaju da je validacija prosledjenih parametara na odredištu uspešna, sa odredišta se u izlaznim parametrima funkcije *OpenSession* vraća isti skup ključeva i potpisa, te se i na pozivnoj strani obavlja provera istih. U slučaju neuspešnog izvršenja bilo kog od opisanih koraka validacije, prekida se proces uspostavljanja sesije, a informacija o razlogu greške se upisuje u lokalnu bazu podataka. Po uspešnom uspostavljanju sesije, odredištu se šalje enkriptovan *SymKey* i potpis poruke, a zatim i paketi poruke. Na prijemu, za svaki paket se proverava identifikator sesije, nakon čega se paket snima u lokalnu bazu. Pošto su svi paketi preneti, sesija se zatvara.

Komponenta *Message Coupler* preuzima primljene pakete i izvršava operacije spajanja paketa u poruku, dekripcije sa simetričnim ključem *SymKey* i dekompresiju. Pošto je poruka rekonstruisana, proverava se potpis poruke i u slučaju uspešne provere, poruka se upisuje u tabelu primljenih poruka odakle će je komponente eksternog sistema, pozivom metode *GetReceivedMessage()* na *External Web Interface* servisu preuzeti za dalju obradu.

Ovakvim načinom prenosa podataka omogućeno je sledeće:

- Obostrana autentifikacija pri uspostavljanju komunikacije
- Enkripcija podataka koji se prenose
- Logovanje svih sesija komunikacije
- Paketizacija poruka
- Momentalan odziv na zahtev za slanje

Cloud okruženje

Zaštita podataka je jedan od najznačajnijih aspekata rada u Cloud okruženju. Ovo proizilazi iz činjenice da upravljamo samo podacima i aplikacijama, dok je potpuna kontrola platforme u rukama provajdera. Kao rezultat neophodno je osiguranje da su naši podaci i aplikacije zaštićeni čak i od strane administratora provider-a.

Kao alat za deploy, upravljanje i praćenje aplikacija i servisa korišćen je Windows Azure Platorm Management Portal. Ovaj portal je Silverlight aplikacija[1] koja koristi SSL[2] za zaštitu komunikacije, a autentikuje korisnike korišćenjem Windows Live ID-a. Windows Live ID je Microsoft-ov Identity provider [3] [4]. Ovako formiran kanal obezbeđuje tajnost podataka koji kroz njega putuju. Sigurnost podataka vezanih za Windows Live ID nalog isključivo je domen vlasnika naloga i zato je neophodno preduzeti adekvatne mere zaštite.

Zaštita podataka u prenosu do Cloud okruženja

Za siguran prenos podataka od AMR centra do Cloud okruženja korišćen je Microsoft SQL Azure Data Sync servis (5). Ovaj servis služi za sinhronizaciju podataka i je formiran na osnovama Microsoft Sync Framework-a. Servis omogućuje dvosmernu sinhronizaciju podataka između više SQL Azure baza podataka koje su razmeštene po različitim “Data centrima” i između SQL Server-a i SQL Azure baza podataka. Za korišćenje ovog servisa potrebno je:

---

[1] Microsoft *Silverlight* je framework za razvoj i rad RIA. RIA (Rich Internet Application) je web aplikacija koja ima mnoge karakteristike windows aplikacije.

[2] SSL (Secure Sockets Layer) je standard i tehnologija za formiranje enkriptovanog kanala komunikacije između web servera i klijenta

[3] Identity provider je servis koji obezbeđuje kreranje, održavanje i upravljanje podacima vezanim za identitet korisnika i omogućuje mu autentikaciju na druge servise unutar federacije

[4] Federacija predstavlja vezu zasnovanu na poverenju između skupa provider-a identiteta i/ili provider-a servisa

- kreiranje SQL Server-a na Azuru,
- konfigurisanje sigurnosnih mehanizama pristupa istom,
- kreiranje baze podataka na prethodno kreiranom serveru i odgovarajućeg administratorskog naloga,
- formiranje Sync grupe[5] u okviru Data Sync servisa,
- migracija neophodnih objekata baze podataka sa SQL server-a AMR Centra na novokreiranu bazu na Azuru. Za potrebe migracije korišćen je SQL Azure Migration Wizard (6).
- mapiranje objekata koji se sinhronizuju
- definisanje učestalosti sinhronizacije

SQL Azure Data Sync omogućuje zaštitu podataka kroz enkripciju i autentikaciju. Enkripciju sprovodi Azure Data Sync servis nad osetljivim podacima koje čuva i koristi. Podaci uključuju kredencijale za pristup sistemskim i korisničkim bazama podataka, kredencijale za pristup sistemskom storage-u kao i konfiguracioni file Data Sync client agent-a. Pored ovoga, svi kanali komunikacije između servisa i komponenti koje se koriste u procesu sinhronizacije su enkriptovani (SSL).

Autentikacija se u okviru procesa sinhronizacije obavlja na nekoliko nivoa:

- Client Agent
    - Data Sync client agent autentikuje korisnika koji mu pristupa preko Windows autentikacije
    - Cloud Data Sync servis authentikuje Data Sync client agent-a ključem agenta koji je jedinstven a generiše se prilikom registracije agenta
- Pristup bazi podataka - korisnikova SQL Server baza podataka autentikuje Data Sync client agent-a koristeći parametre konekcije i kredencijale koje korisnik obezbeđuje, a podrazumevaju SQL Server username/password.
- Sistemske komponente – digitalni sertifikati se koriste za autentikaciju unutar Cloud servis sistema.

Zaštita podataka na Cloud okruženju

Zaštita podataka na Cloud okruženju obezbeđena je kroz zaštitu pristupa podacima kao i zaštitu kanala za pristup podacima.

SQL Azure Pristup podacima na Azure SQL Serveru kontrolisan je kroz dva tipa kontrole pristupa: SQL Srver autentikacija[6] i SQL Azure Firewall. Pored ovog, obezbeđena je zaštita kanala komunikacije kroz SQL Server's protocol enkripciju (svi podaci koji se razmenjuju sa SQL Server-om prolaze kroz SSL-om enkriptovani kanal komunikacije). Za aplikativni pristup podacima formiran je korisnički nalog čiji se kredencijali čuvaju u konfiguracionom file-u aplikacija/servisa zaštićeni (enkriptovani) ključem storage-a na kome se aplikacija nalazi. Ovaj korisnički nalog ima samo pravo izvršenja odgovarajućih procedura neophodnih za funkcionalnost aplikacija/servisa. SQL Azure Firewall omogućava definisanje skupa dozvoljenih IP adresa odnosno adresnih opsega sa kojih može da se pristupi aplikaciji. Dodatno je sva komunikacija između SQL Azure-a i klijentskih aplikacija/servisa zaštićena korišćenjem SSL-a.

[5] Sync grupa predstavlja skup baza podataka koje su logički povezaneu svrhu sinhronizacije podataka.

[6] SQL Server autentikacija podrazumeva postojanje korisničkog naloga formiranog na SQL Server-u sa čijim je kredencijalima (login id/password) dozvoljena autentikacija.

SQL Azure Reporting Kao jedan od načina za publikovanje podataka prikupljenih u AMR Centru korišćen je Azure SQL Reporting Service za hostovanje i Report Viewer[7] kontrola za prikaz podataka preko web aplikacije WEBReports. Azure SQL Reporting dozvoljava samo SQL Azure username/password autentikaciju i upravljanje pravima pristupa izveštajima preko rola. Zbog toga je kreiran poseban nalog za publikovane izveštaje koji ima pravo izvršavanja upita samo nad odgovarajućim skupom podataka. Kredencijali ovog naloga su zaštićeni (enkriptovani) ključem storage-a na kom je hostovana WEBReports aplikacija.
Autentikacija na aplikacije i servise hostovane na Cloud-u Kada govorimo o autentikaciji na aplikaciju, korisnici mogu da se nađu u dve role. Svim korisnicima obezbeđena je autentikacija preko eksternog autentikacionog provajder-a (Janrain Engage), dok je administratorskoj roli dodata mogućnost autentikacije preko username/password-a.

Kontrola i zaštita pristupa podacima preko servisa i aplikacija na Cloud-u vrši se autentikacijom. Autentikacija je konfigurisana, prema nameni, korišćenjem:

- digitalnih sertifikata, kada je namena unutar Cloud platforme
- claim-ova, korišćenjem eksternih autentikacionih provider-a, kada je namena izvan granica Cloud-a

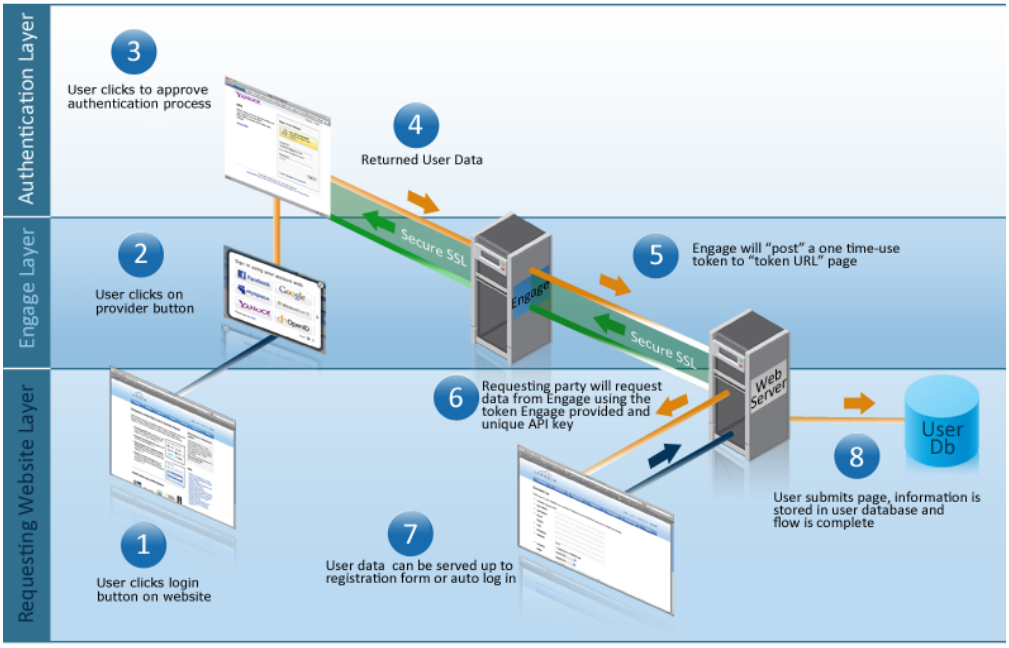
Dodatno, sva komunikacija sa servisima ostvarena je korišćenjem SSL-a.

Autentikacija putem digitalnih sertifikata je korišćena preko pravila mapiranja “many-to-one“ koje je konfigurisano tako da omogućuje pristup svim sertifikatima izdatim od strane CA[8] koji je vlasnik pretplate na Microsoft Azure platformu u okviru koje se nalaze komponente SESAME-S sistema. Kao eksterni autentikacioni provider-i korišćeni su Janrain Engage i Microsoft Azure ACS.Janrain Engage, kao deo Janrain[9] platforme, je komponenta za registraciju i logovanje korisnika korišćenjem svojih “social web” identiteta. Naš sistem dozvoljava Google, Yahoo i Windows Live ID kao eksterne provajdere identiteta. Ovaj modul integrisan je u Drupal site (Alphaverda) koji se nalazi na Cloud-u i omogućuje registraciju i logovanje korisnika aplikacije koje prikazuje slika 3.

[7] Komponenta .Net framework-a koja omoućuje autentikaciju i prikaz izveštaja generisanih preko SQL Reporting servisa

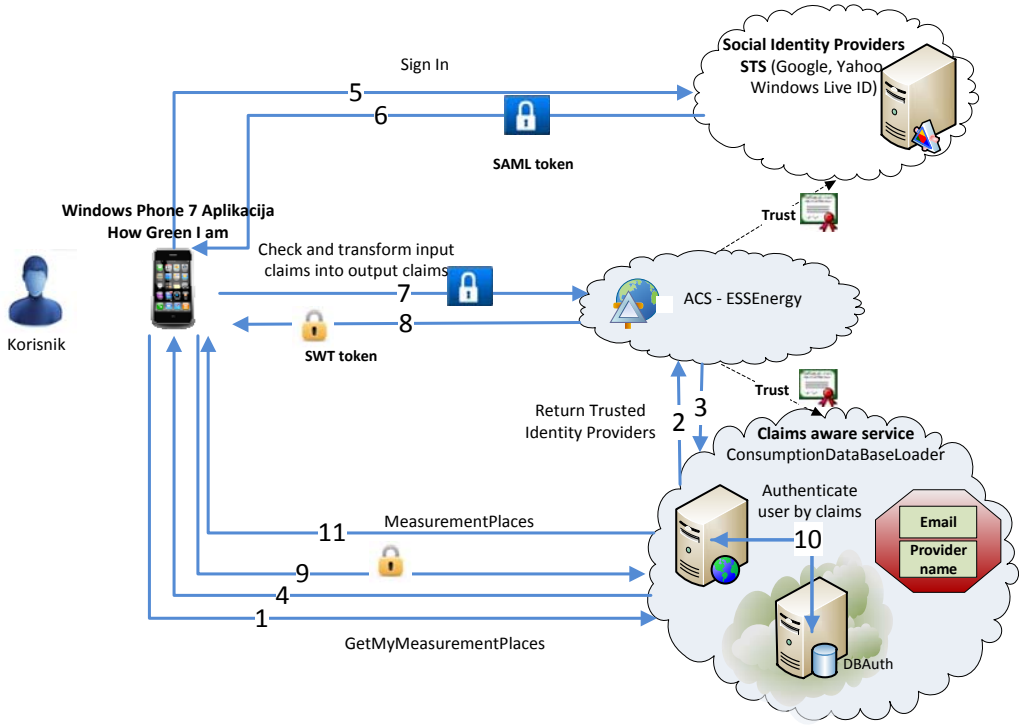
[8] Certificaion Authority je entitet koji izdaje i upravlja digitalnim sertifikatima

[9] Janrain je SaaS (software as a service) platforma. Detajnije o SaaS platformi u (7)



Slika 3 – Proces registracije/logovanja preko Janrain engage modula

Za autentikaciju na servise korišćenjem istih eksternih provajdera identiteta, iskorišćen je Azure Access Control Service (8). Preko ACS-a je dozvoljeno samo logovanje prethodno registrovanjih korisnika preko Alphaverda aplikacije.



Slika 4 – Proces logovanja preko ACS-a

ZAKLJUČAK

U vremenu kada je implementacija Smart Metering i Smart Grid koncepata u svetu dostigla tačku gde se poseban akcenat daje sigurnosti podataka i zaštiti privatnosti fizičkih i pravnih lica, neophodno je obezbediti maksimalnu zaštitu svih osetljivih podataka. Opisanim rešenjem zaštićeno je nekoliko tačaka i komunikacionih puteva između njih na relaciji Brojilo – Servisni portal za korisnika. Za realizaciju ove zaštite korišćeni su postojeći mehanizmi, dostupni u paleti Microsoft proizvoda, i novokreirani mehanizmi koje smo razvili kako bi zaštitili put od Koncentratora do AMM Centra.

LITERATURA

[1] European Commision: Climate Action. 2007. (http://ec.europa.eu/clima/policies/package/index_en.htm)

[2] JP „Elektroprivreda Srbije“, *Funkcionalni zahtevi i tehničke specifikacije AMI/MDM sistema*, Beograd, 2010. (http://www.eps.rs/publikacije/interni_standardi/20052010/AMI_MDM_Konacno.pdf)

[3] www.dlms.com

[4] Short introduction to Cloud Platforms, 2008. (http://www.davidchappell.com/CloudPlatforms--Chappell.pdf)

[5] SQL Azure Data Sync, Microsoft MSDN, http://msdn.microsoft.com/en-us/library/hh456371.aspx

[6] SQL Azure Migration Wizard documentation,CodePlex, http://sqlazuremw.codeplex.com/documentation

[7] Janrain Engage Flow,Janrain, https://rpxnow.com/docs

[8] ACS Functionality, Microsoft MSDN, http://msdn.microsoft.com/en-us/library/windowsazure/gg185966.aspx

Milan Stefanović, dipl Mat.
E-Smart Systems d.o.o, Kneza Višeslava 70A, 11030 Beograd
tel: +381 11 3050200

Vladimir Pejović, dipl ing. elektrotehnike
E-Smart Systems d.o.o, Kneza Višeslava 70A, 11030 Beograd
tel: +381 11 3050200

Vanja Bajić, dipl ing. organizacionih nauka
E-Smart Systems d.o.o, Kneza Višeslava 70A, 11030 Beograd
tel: +381 11 3050200

Mirna Kojić Veljović, mag. eletrotehnike
E-Smart Systems d.o.o, Kneza Višeslava 70A, 11030 Beograd
tel: +381 11 3050200