Nabava sustava za automatizirano upravljanje mobilnim uređajima

-

MDM (Mobile Device Management)

TEHNIČKA SPECIFIKACIJA

Sadržaj:

Uvod

Predmet nabave je izrada softvera za rješenje za automatizirano upravljanje mobilnim uređajima (eng. MDM - Mobile Device Management) u sklopu II. faze programa „e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće“, u daljnjem tekstu Rješenje.

Nabava podrazumijeva:

- Izradu softvera za rješenje za upravljanje mobilnim uređajima,
- Usluge potrebne za njegovu implementaciju na infrastrukturi Naručitelja
- Operativnu podršku i brigu o sustavu tokom trajanja II. faze programa
- Dodatne prilagodbe Rješenja kako bi se zadovoljili svi uvjeti i potrebe Naručitelja za upravljanje mobilnim uređajima.
- Usluga produženog jamstva za ispravnost isporučenost rješenje tokom minimalno 5 godina nakon završetka projekta

Specifikacija predmeta nabave

Rješenje mora omogućiti centralizirano upravljanje mobilnim uređajima Naručitelja, prikupljanje informacija s uređaja, postavljanje sigurnosnih postavki, distribuciju i upravljanje mobilnim aplikacijama te distribuciju i upravljanje dokumentima.

Obzirom da svi korisnici mobilnih uređaja iz projekta e-Škole posjeduju elektronički identitet u sklopu AAI@EduHr sustava, Rješenje se mora integrirati sa navedenim (AAI@EduHr je autentikacijska i autorizacijska infrastruktura sustava znanosti i obrazovanja u Republici Hrvatskoj).

Rješenje mora omogućavati prijavu korisničkih uređaja u MDM sustav bez potrebe dolaska korisnika na centralnu lokaciju. Svi eventualni dodatni troškovi (materijalni ili vremenski) vezani uz prijavu uređaja u sustav i naknadnu konfiguraciju moraju biti osigurani od strane Ponuditelja.

Rješenje mora podržavati mogućnost opsluživanja i kreiranja višestrukih organizacija eng. Multitenat) s različitim postavkama, integracijskim parametrima i administracijskim pravima za svaku kreiranu organizaciju unutar sustava.

Ponuđeno rješenje mora imati mogućnosti: vizualne prilagodbe korisničkog i administracijskog dijela sustava organizaciji Naručitelja (knjiga grafičkih standarda Naručitelja) te integracije sa postojećim sustavima i aplikacijama Naručitelja preko programskog sučelja (REST-API) za povezivanje aplikacija Naručitelja sa MDM rješenjem.

Potrebno je omogućiti kontrolu učlanjivanja mobilnog uređaja u MDM sustav, koji treba biti dozvoljena samo za one mobilne uređaje koji su upisani u bazu ili aplikaciju odobrenih mobilnih uređaja Naručitelja.

Traženo Rješenje se mora ponuditi sa pravima na trajno korištenje sustava (tzv. perpetual license) uz pravo na nadogradnje na nove verzije sustava tokom trajanja projekta i za vrijeme jamstvenog perioda, uz mogućnost produženja prava na nadogradnju na sljedeće godine, za što Ponuditelj treba istaknuti cijenu produženja nadogradnji.

Isporuke i dinamika plaćanja

Rješenje mora podržavati ukupno do 250 000 uređaja koji se mogu prijaviti u MDM sustav.

Očekivana dinamika uključivanja uređaja u MDM sustav je u tri faze, sa sljedećim rokovima:

- Faza 1. - do 100.000 uređaja do kraja 2019. godine
- Faza 2. - do 200.000 uređaja do kraja 2020. godine
- Faza 3. - do 250.000 uređaja do kraja 2021. godine

Traženo rješenje od početka rada treba biti skalabilno i dimenzionirano za uključenje novih ustanova i povećanje broja uređaja, a povećanje broja uređaja do predviđenog maksimalnog broja ne smije utjecati na performanse, funkcionalnosti i ukupan trošak korištenja rješenja.

Dinamika plaćanja će biti godišnja i pratiti će očekivane Faze uključivanja uređaja.

Smještaj

Rješenje je potrebno u potpunosti primijeniti u okolini Naručitelja (eng. On-Premise). Rješenje je potrebno realizirati s posebnim naglaskom na pouzdanost, skalabilnost, visoku dostupnost i sigurnost.

Naručitelj će za potrebe MDM rješenja osigurati testnu i produkcijsku kontejner platformu.

Programski kod

Za traženo Rješenje očekuje se da Ponuditelj osigura uvid u programski kod te da se izvorni programski kod MDM rješenja pohrani na Naručiteljevom repozitoriju koda. Ujedno Ponuditelj mora osigurati mogućnost promjene programskog koda MDM rješenja prema potrebama i na zahtjev Naručitelja. Ponuditelj je također dužan osigurati da se sve promjene na produkcijskoj verziju sustava šalju isključivo sa Naručiteljevog repozitorija koda. Ponuditelj je dužan posebnom izjavom potvrditi da će osigurati uvid u izvorni programski kod ponuđenog Rješenja i pohranu istog kod Naručitelja kao i da je u stanju osigurati promjene koda na zahtjev Naručitelja.

Jezik

Korisničko sučelje ponuđenog Rješenja za prijavu uređaja u sustav i korisnički samouslužni portal trebaju biti dostupni na hrvatskom jeziku, kao i sva administracijska sučelja.

Funkcijska specifikacija Rješenja

Integracije

Zahtjevi kod integracije se odnose na postojeće tehnologije kod Naručitelja i podrške najnovijim verzijama programske podrške (operativnih sustava, baze podataka, PKI rješenja i sl.).

- Podrška za poslužiteljski operativni sustav otvorenog koda
- Podrška za protokole (SAML2, OAuth, LDAP)
- Podrška za povezivanje na „Cloud“ imeničke servise Office365, Azure AD, Google Apps ID
- Podrška za PostgreSQL bazu podataka

Ponuditelj mora uključiti u ponudu shemu arhitekture sustava sa mogućnostima instalacije komponenti sustava u različite mrežne segmente (npr. U tzv demilitarizirano sigurnosnu zonu).

Opće funkcionalnosti

- Mogućnost provjera ulaska uređaja u sustav – kontrola serijskog broja uređaja prilikom prijave uređaja u sustav (nakon ulaska uređaja u sustav prikazati za svaki pojedini uređaj ID uređaja, korisničko ime, operativni sustav, oznaka uređaja, IMEI broj, serijski broj, model, prva prijava u sustav, zadnja akcija na uređaju)
- Automatizacija administracije sustava – kreiranje administratorskih poslova (liste naredbi) i njihova automatizaciju (tj. izvođenje zadataka za određene grupe uređaja u određenim vremenskim intervalima/terminima)
- Korisnički samouslužni (Self-service) portal za krajnje korisnike s mogućnošću samostalnog izvršenja administrativnih zadataka na mobilnom uređaju (npr. instalacije konfiguracijskih profila, instalacije i nadogradnja aplikacija, izvođenje interventnih naredbi i sl.)
- „Multi tenant“ podrška – mogućnost opsluživanja i kreiranja višestrukih organizacija sa u cijelosti različitim MDM postavkama, integracijskim parametrima i administracijskim pravima bazirana na tkzv. „Multitenat“ arhitekturu
- Mogućnost dodjeljivanja korisnicima raznih korisničkih uloga. Primjer uloga: super administrator, administrator organizacije, tehničar, revizor, korisnik uređaja ili druge uloge po potrebama Naručitelja.
- Fleksibilna primjena prava koje MDM sustav ima za razne grupe mobilnih uređaja.

- MDM sustav mora podržavati sljedeće operativne sustave: Android 8.0 ili IOS 11 ili Windows 10 OEM ili Chrome OS 73 ili Linux OS

Zahtjevi prema upravljačkom sučelju

- Stvaranje dinamičkih grupa uređaja po atributima uređaja
- Preuzimanje podatka o mobilnim uređajima u CSV datoteku sa mogućnosti prilagodbe skupa atributa
- Prilagodljiv sustav za izvještavanje i dodatni detaljni uvid u upotrebu mobilnih uređaja
    - ukupan broj uređaja unutar MDM sustava,
    - broj uređaja po pojedinoj školi,
    - modeli uređaja u sustavu,
    - verzija operativnog sustava na pojedinom uređaju,
    - vrsta SIM kartice na pojedinom uređaju,
    - prikaz verzije MDM sustava po uređaju,
    - prikaz instaliranih profila i restrikcija po pojedinom uređaju,
    - semafor aktivnosti mobilnih uređaja,
    - potrošnja prometa po SIM kartici,
    - po pojedinoj aplikaciji te po bežičnoj mreži,
    - vremenska crta instaliranih aplikacija na uređaju te njihove verzije,
    - vremenska crta instaliranih aplikacija koje su instalirane na uređaje centraliziranim putem,
    - vremenski prikaz korištenja pojedinih aplikacija,
    - stanje kapaciteta memorije i razina napunjenosti baterije na pojedinom uređaju.

Opće funkcionalnosti

- Mogućnost provjera ulaska uređaja u sustav – kontrola serijskog broja uređaja prilikom prijave uređaja u sustav (nakon ulaska uređaja u sustav prikazati za svaki pojedini uređaj ID uređaja, korisničko ime, operativni sustav, oznaka uređaja, IMEI broj, serijski broj, model, prva prijava u sustav, zadnja akcija na uređaju)
- Automatizacija administracije sustava – kreiranje administratorskih poslova (liste naredbi) i njihova automatizaciju (tj. izvođenje zadataka za određene grupe uređaja u određenim vremenskim intervalima/terminima)
- Korisnički samouslužni (Self-service) portal za krajnje korisnike s mogućnošću samostalnog izvršenja administrativnih zadataka na mobilnom uređaju (npr. instalacije

konfiguracijskih profila, instalacije i nadogradnja aplikacija, izvođenje interventnih naredbi i sl.)

- „Multi tenant“ podrška – mogućnost opsluživanja i kreiranja višestrukih organizacija sa u cijelosti različitim MDM postavkama, integracijskim parametrima i administracijskim pravima bazirana na tzv. „Multitenat“ arhitekturu
- Mogućnost dodjeljivanja korisnicima raznih korisničkih uloga. Primjer uloga: super administrator, administrator organizacije, tehničar, revizor, korisnik uređaja ili druge uloge po potrebama Naručitelja.
- Fleksibilna primjena prava koje MDM sustav ima za razne grupe mobilnih uređaja.
- MDM sustav mora podržavati sljedeće operativne sustave: Android, iOS, Windows

Sigurnosni zahtjevi sustava

- Podrška za jednokratne lozinke (OTP) – generiranje jednokratne lozinke sa ograničenim vremenom trajanja za korisnike i prijava uređaja u sustav putem iste
- Dvofaktorska autentikacija – mogućnost dvofaktorske autentifikacije kod prijave korisnika u sustav ili u neke njegove dijelove (admin konzolu ili samouslužni portal). Obavezna podrška za javne 2-factor autentikacijske sustave (Google i Microsoft Authenticator), podrška za ADFS Multifactor, te mogućnost prilagodbe rješenja za druge OTP servere i fizičke tokene
- Prijava uređaja u sustav (Enrollment), putem korisničkog imena, lozinke ili OTP koda
- Definiranje i nametanje politike za lozinke (Password policy)

Sigurnosni zahtjevi u postavka uređaja

- Mogućnosti zaključavanja uređaja
- Mogućnost udaljenog privremenog uklanjanja lozinke (PIN-a) uređaja
- Udaljeno brisanja uređaja (Factory Reset)
- Selektivnog brisanja poslovnih aplikacija, dokumenta i postavki sa uređaja

Povećanje produktivnosti i korisničke postavke uređaja

- Mogućnost postavljanja „prečaca“ sa URL vezama (tkzv. WebClip) na radnu površinu uređaja
- Mogućnost zabrane promjene određenih postavki na uređajima
- Kontrola zabrane instalacije i deinstalacije programa od strane korisnika

- Kontrola zabrane mogućnosti instalacije programa sa službenih stranica za instalaciju (AppStore , GooglePlay ili neovisnih izvora)

SSO-a prijava

- Podrška za siguran pristup putem SSO (Single Sign On) prijave korisnika internim portalima i web aplikacijama
- Podrška za Client Certificate SSL autentikaciju na Web aplikacije i portale iz preglednika na mobilnim uređajima

Upravljanje e-poštom na mobilnom uređaju

- Automatska konfiguracija korisničkog računa u e-mail aplikacije na mobilnim uređajima koji to podržavaju

Podrška za bežične mreže (Wi-Fi)

- Podrška za WPA2-Enterprise i WPA2 Personal
- Podrška za kreiranje konfiguracijskih profila sa autentikacijskim protokolima:
    - PEAP
    - EAP-TLS (putem korisničkog certifikata)

Upravljanje mobilnim aplikacijama (eng. Mobile Application Management - MAM)

- Instalacija, nadogradnja i uklanjanje mobilnih aplikacija
- Podrška za „javne“ aplikacije s javnih servisa (Google Play, iTunes)
- Podrška za „Enterprise“ aplikacije razvijene od strane Naručitelja i partnera
- Mogućnost konfiguracije i komunikacije mobilnih „Enterprise“ aplikacija i MDM sustava (kroz unaprijed definiran model)

Upravljanje datotekama

- Udaljena i centralizirana distribucija datoteka (npr. pdf dokumenata)
- Mogućnost ažuriranja i uklanjanja datoteka
- Automatsko uklanjanje upravljanih datoteka prilikom izlaska uređaja iz MDM sustava

Podrška sigurnosnim mobilnim tehnologijama drugih proizvođača

- Podrška za Samsung „KNOX Workspace“
- Podrška za Google „Android for Work“

Operativnu podršku i brigu o sustavu tokom trajanja II. faze programa

Operativna podrška uključuje otklanjanje uzroka zastoja i neispravnosti u radu sustava i svih njegovih elemenata (eng. bug). Ponuditelj treba pružati uslugu po prijavi zastoja ili neispravnosti u radu od strane CARNET-a ili ovlaštenog predstavnika CARNET-a.

Operativna podrška aplikacijskog rješenja obavlja se u režimu 12x5, odnosno 12 sati svaki radni dan u godini s vremenom odziva četiri sata od prijave incidenta ili "sljedeći radni dan" za incidente prijavljene vikendom/neradnim danom, i vremenom popravka kontinuiranim do ispravka prijave.

Poslovi i aktivnosti operativne podrške obuhvaćaju praćenje i podešavanje svih parametara sustava. Ponuditelj periodički provjerava rad sustava i preventivno obavlja sve potrebne akcije kako bi sustav uvijek ispravno radio. Navedeno podrazumijeva tjedni pregled stanja sustava.

Jednom u tri mjeseca ponuditelj treba podnositi izvještaj o stanju informacijskog sustava uz prijedlog za eventualne promjene konfiguracije kako bi se osigurala pouzdanost, optimalan rad i funkcionalnost sustava. Naručitelj može zatražiti i izvanredni (ad-hoc) izvještaj o stanju sustava kojeg ponuditelj mora izraditi i dostaviti Naručitelju.

Operativna podrška i briga o sustavu obuhvaća:

- intervencije u slučajevima kada informacijski sustav ne radi prema zadanoj specifikaciji,
- intervencije na komponentama sustava primjenom zakrpa,
- intervencije vezane za konfiguracijske parametre komponenta sustava
- kontinuirani nadzor rada softvera,
- pregled postavki sustava, pregled rada aplikacijskog poslužitelja,
- pregledavanje rada baze podataka,
- nadzor i optimizacija performansi,
- pripremu i podršku sustava za sigurnosno testiranje koje provodi CARNET ili ovlašteni predstavnik CARNET-a,
- redovito sigurnosno nadograđivanje sustava sa zakrpama proizvođača softvera u skladu s preporukama i dobrim praksama proizvođača.

Implementacija zakrpa (engl. patch) nužno je napraviti u roku od 2 tjedna od izdavanja zakrpe od strane proizvođača. U slučajevima pojave kritičnih sigurnosnih problema (engl. Zero-Day Vulnerability) koji bi ugrozili sustav i podatke pohranjene na sustavu zakrpe treba implementirati odmah bez odgađanja.

Sigurnosno testiranje

Nakon izrade svih funkcionalnosti sustava, a prije stavljanja u produkcijsko okruženje odabrani ponuditelj dužan je omogućiti Naručitelju provođenje sigurnosnog testiranja.

Postupak sigurnosnog ispitivanja podrazumijeva detekciju eventualnih sigurnosnih propusta u aplikaciji automatiziranom analizom i korištenjem specijaliziranih alata te ručne provjere sigurnosnih postavki.

Ponuditelj treba osigurati da je isporučen sustav i svi njegovi elementi u skladu s OWASP Application Security Verification Standard 3.0 – poželjno Level 3, a najmanje Level 2 (https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf).

Sigurnosno testiranje obavljat će Naručitelj, a odabrani Ponuditelj dužan je omogućiti zahtijevano provođenje sigurnosnog testiranja od strane Naručitelja. Odabrani Ponuditelj sukladno rezultatima testiranja obavezan je poduzeti adekvatne mjere za ispravljanje sigurnosnih propusta u vremenu definiranom u mjeri za ispravljanje propusta.

U svrhu sigurnosnog testiranja, ponuditelj je dužan omogućiti:

- provođenje testiranja od strane Naručitelja
- sukladno rezultatima testiranja poduzeti adekvatne mjere za ispravljanje sigurnosnih propusta
- prilagodbu testne okoline koja treba biti identična produkcijskoj (pri čemu verzija aplikacije treba biti sukladna onoj koja će se koristiti u produkciji) s „root“ (administratorskim) pristupom na sustav
- korisničke račune za sve uloge koje postoje u aplikaciji
- pristup produkcijskom sustavu kako bi mogla biti izvršena provjera konfiguracija sustava s „root“ (administratorskim) pristupom
- izvorni kod sustava
- ažurnu tehničku dokumentaciju sustava

Odabrani Ponuditelj će o svom trošku poduzeti adekvatne mjere i sigurnosne ispravke sukladno zahtjevu i u roku dogovorenim sa Naručiteljem. Naručitelj može ponoviti testiranje sve do otklanjanja i ispravljanje sigurnosnih propusta.

Osim prije inicijalnog postavljanja aplikacije u produkcijsku okolinu, testiranje će se provoditi: periodički (minimalno jednom godišnje za vrijeme trajanja ugovora) te izvanredno (na zahtjev, u slučaju veće nadogradnje sustava ili u slučaju sigurnosnog incidenta).

Usklađenosti s općom uredbom o zaštiti osobnih podataka (GDPR)

Isporučena usluga mora biti u skladu s Općom uredbom o zaštiti osobnih podataka (Uredba (EU) 2016/679) te primjenjivati metode i principe dizajna sustava i zaštite osobnih podataka koje Uredba propisuje.

Vlasništvo nad izvornim kodom i korisnička dokumentacija

Vlasništvo nad izvornim kodom, te pripadajućom razvojnom, tehničkom i korisničkom dokumentacijom Ponuditelj je obvezan, nakon uspješne primopredaje sustava sa svim traženim funkcionalnostima, prenijeti na Naručitelja, te mu predati u posjed izvorni kod programskog rješenja i sve potrebne programske biblioteke programske platforme za dalji razvoj isporučenih aplikacija u strojnom kodu i pripadajuću dokumentaciju i time prenijeti na Naručitelja pravo modifikacije i daljnjega razvoja programskog rješenja.

Naručitelj može koristiti izvorni kod programskog rješenja i programsku platformu za razvoj drugih aplikacija. Ponuditelj zadržava pravo daljeg korištenja izvornog koda, te ima pravo isti koristiti za dalji razvoj vlastitog rješenja.

Ponuditelj je obavezan predati Naručitelju korisničku dokumentaciju koja uključuje:

- funkcionalnosti sustava - popis ključnih funkcionalnosti i namjena (opis funkcionalnosti)
- nefunkcionalni opis sustava - računalna platforma (klijentska razina, poslužiteljska razina), performanse i raspoloživost, sigurnost, komunikacija s vanjskim sustavima, dizajn sučelja i slično
- arhitekturu sustava i opis modela podataka - aplikativna arhitektura sustava (platforma, klijentska razina - prezentacijski i servisni sloj, poslužiteljska razina - servisni i podatkovni sloj), izvedbena arhitektura sustava (servisni i podatkovni sloj - broj poslužitelja, VM, fizički poslužitelji, zaštita sustava, međusobna povezanost, ...), okoline i instance sustava (razvojna, testna i produkcijska okolina)
- korištene tehnologije i razvojni alati - popis tehnologija i alata, te vrsta i namjena
- upute za administratore sustava
- upute za korisnike - upute za različite uloge korisnika

Komunikacija na projektu i nadzor provedbe ugovora

Naručitelj će kontinuirano pratiti provedbu ugovorene usluge te je stoga odabrani ponuditelj dužan omogućiti Naručitelju pravovremeni i redoviti uvid u sve aktivnosti koje će se provoditi po ugovoru sklopljenom na temelju ovog procesa javne nabave. Nadalje, odabrani Ponuditelj treba Naručitelju omogućiti neposredan uvid u rad stručnjaka i rezultate u svakom trenutku provedbe ugovorenih usluga.

Naručitelj će za potrebe razvoja sadržaja i praćenja napretka provedbe osigurati potrebnu računalnu infrastrukturu za produkcijsku i testnu okolina, koja će ponuditelju omogućiti redovno dostavljanje sadržaja u razvoju odnosno programskog koda u repozitorij koda i u odgovarajuću okolinu.

Naručitelj će osigurati i zahtijevati propisani kanal komunikacije između tehničkih osoba radi preuzimanja zahtjeva za izmjenama i ispravkama uočenih grešaka ili nedostataka u izrađenom sadržaju.

Praćenje napretka provedbe od strane Naručitelja odvija se putem i redovitog izvještavanja putem redovitih status sastanaka imenovanih voditelja projekta Naručitelja i Ponuditelja, minimalno jednom u dva tjedna tokom implementacije rješenja.

Neposrednim uvidom u rad stručnjaka i rezultate u svakom trenutku provedbe ugovorenih usluga, Naručitelj će pratiti napredak provedbe ugovora.

Po uvidu Naručitelja u rad odabranog ponuditelja, Naručitelj ima pravo dati komentare na rad i rezultate odabranog ponuditelja. Odabrani ponuditelj dužan je usvojiti komentare u postavljenom roku definiranom u skladu s dogovorom s Naručiteljem.