Насоки за техничките барања, начин на работа и функционирање на комуникацискиот клиент и препораки за користење на системот за интероперабилност

1 Технички барања во однос на хардверската и софтверската инфраструктура на комуникацискиот клиент

Секоја институција со обемен број на корисници за да може да биде препознаена од системот за интероперабилност е потребно да поседува Комуникациски клиент.

1.1 Комуникациски клиент

Комуникациски клиент (К-Клиент) е хардверски уред со соодветен софтвер, кој обезбедува интерфејс за размена на документи и податоци во електронска форма кои се разменуваат меѓу информациските системи на органите кои учествуваат во размената.

Комуникацискиот клиент доколку во својот состав поседува и компјутерска компонента мора да биде приклучен на активен доменски директориумски сервис што е засебно конфигуриран за потребите на Интероперабилност. Оперативниот систем на компјутерскиот дел од К-клиентот треба да е способен да се приклучи на доменот на интероперабилност.

К-клиентот комуницира со информацискиот систем на институцијата од една страна и со централниот Комуникациски сервер од другата страна.

К-клиентот е потребно да биде поврзан со Комуникацискиот сервер преку Виртуелна привтна мрежна (VPN) конекција.

Хардверската конфигурација на компјутерскиот дел на К-клиентот ја одредува секоја институција засебно и е во зависност од протокот на информациите што минуваат низ него.

К-клиентот треба да е способен да комуницира преку веб сервиси со Информацискиот систем на институцијата и Комуникацискиот сервер на системот за интероперабилност.

Работењето и функционирањето на комуникацискиот клиент е исклучиво наменето за потребите на размена на информации меѓу институциите во рамки на Интероперабилноста.

К-клиентот учествува директно во размената на пораки и е поврзан со мрежата на институцијата.

Секоја институција е должна и одговорна да го одржува сопствениот комуникациски клиент.

Одржувањето особено ги опфаќа следните карактеристики:

- За хардверската опрема е потребно е да бидат обезбедени сите физички услови според спецификацијата на производителот, соодветна температура, влажност на воздухот, електрично напојување, просторни услови и др.
- потребно е да се извршува редовен мониторинг, преглед на логовите кои ја опишуваат работата на комуникацискиот клиент, проверка за функционалност, безбедносни проверки и др.

1.2 Мрежна инфраструктура

Како мрежна инфраструктура на системот за интероперабилност се користи затворена внатрешна мрежа, базирана на оптички влакна како преносен медиум, преку која се пристапува до Комуникацискиот сервер.

Доколку до рамките на органот не постои соодветна оптичка мрежна инфраструктура тогаш е потребно на К-клиентот да му се обезбеди интернет конекција преку која со помош на ВПН конекција ќе комуницира со Комуникацискиот сервер. За оваа намена на К-клиентот му е потребна јавна IP адреса.

Како уред за рутирање може да се користи било кој уред што е способен да формира ВПН конекција со рутерите на Комуникацискиот сервер.

Како пример за препорака е рутерот да ја подржува следната конфигурација:
Routing Protocols RIP v2 ; OSPF ;
Management SSH v2 ; HTTPS ; SYSLOG
Onboard LAN Ports: 2 x Fast Ethernet 10/100

IPSec VPN Advanced Encryption Standard (AES) 128, 192, and 256; Triple Data Encryption Standard (3DES); and DES cryptology support, Embedded hardware-based VPN acceleration on the motherboard, VPN remote server, Dynamic Multipoint VPN (DMVPN), Virtual Tunnel Interfaces (VTI), VPN QoS - Preclassification support.

2 Тестна околина

Секоја институција е должна покрај продукцискатa да одржува и тестна околина, која ќе служи за тестирање и развој на системот за интероперабилност.

Податоците што се користат за размена во рамките на тестната околина не треба да се вистинити туку е потребно да бидат податоци обработени за потреби на тестирање, т.е. не смее да постојат вистински имиња, презимиња или било кои други податоци кои би биле компромитирачки.

3 Одржување, развој и животен век на постоечки веб сервиси

Трајно исклучување на веќе постоечки веб сервис не смее да се изведе без претходно известување и согласност од секторот за интероперабилност во МИОА. Сите засегнати институции кои го користат веб сервисот се должни да достават предлог датум кога е можно сервисот да биде исклучен за да може да се приспособат, но периодот на приспособување не смее да биде подолг од една година.

Привремено исклучување на веќе постоечки веб сервиси за потреби на одржување или други непредвидени дејности е неопходно да биде најавено, а исклучувањето треба да се случува во период вон работното време. Во рамки на работно време можно е да се изведе привремено исклучување, но само по одобрување од страна на корисниците на сервисот и од страна на центарот за интероперабилност во МИОА.

Секое побарување на веб сервис по одредени параметри, во својот одговор покрај останатите параметри како одговор мора да ги содржи и параметрите по кој е повикан.

За секој сервис што го обезбедуваат органите во рамките на системот за интероперабилност се должни да ги достават следните карактеристики за сервисот и тоа:

- Време на одговор на сервисот (минимално, максимално, просечно),
- Рата на грешки,
- Проток (Се мери во бајти и репрезентира количество на информации кои виртуелните корисници ги примаат од серверот во секунда),
- Барања во секунда (колку барања во секунда може да опслужи сервисот),
- Истовремени корисници, и
- Друго.

За секое побарување за користење на сервис на одреден орган од страна на друг орган, органот побарувач е должен до Министерството за информатичко општество и администрација да достави информација за капацитативна потреба од искористување на сервисот, а особено за бројот на истовремени корисници кои ќе го користат сервисот, барања во секунда минута или час и други информации за потребниот капацитет.

4 Електронска пошта

При размена на електронски изјави по електронска пошта да се користи задолжително протоколот SMTP ("Simple Mail Transfer Protocol") основан на Препораки RFC 2821 и 2822, усвоени од IETF (The Internet Engineering Task Force - Целна група за интернет инженеринг) април 2001 г.;

5 Пристап до информации што се разменуваат

Со цел да се пристапи или да се добијат информации од системот за интероперабилност, во рамки на органите е потребно да се користат веб прелистувачи или специфични клиентски апликации кои дозволуваат меѓудругото и директен пристап до Интернет базирани сервиси, сервери за електронска пошта и други ресурси. Употреба на Active-x контроли генерално е забрането.

Веб прелистувачи

Со цел да се овозможи широко распространето користење на еВладини апликации, како front-end уред потребно е да се користи веб прелистувач кој е способен да процесира и презентира формати на презентациско ниво.

Користењето на колачиња е дозволено под следните услови:
- колачињата не се постојани, и
- веб страни на домејн не вклучуваат содржина од други домејни кои поставуваат колачиња.

Користењето на Javascript е дозволено, со тоа што се препорачува веб страните да можат да бидат користени дури и доколку Javascript опцијата да е деактивирана.

Користењето на Java аплети е дозволено ако истите се потпишани од серверот и можат да бидат идентификувани од страна на клиентот како автентицирани и некорумпирани.

6 Безбедност и интегритет

За потребите на безбедност и интегритет на информациите се користи :

- HTTPS протоколот,
- автентификација, авторизација,
- поврзаност во доменска структура,
- VPN конекција,
- користење на дигитални потписи,
- енкрипција на пораките што се разменуваат,
- физичко обезбедување на просторот, и
- други мерки согласно општо прифатените препораки и стандарди за безбедност, ISO 27000 за безбедност и W3C стандардите.

6.1 XML Потпис

W3C и IETF стандард за XML потпис (XML синтакса за потпис и процесирање, W3C препораки и IETF RFC 3275) опишува дигитални потписи за сите видови податоци (најчесто XML) обезбедувајќи XML шема и множество на процесирачки правила (за генерирање и валидирање на потпис). Потписот може да покрие еден или повеќе документи и/или различни видови на податоци (слики, текст, и др.). Една централна карактеристика на XML потписот е дека е возможно да се потпише специфични делови од XML документ а не само цел документ. Благодарение на оваа флексибилност е возможно да се обезбеди интегритет на одредени елементи од XML документот.

6.2 XML Енкрипција

W3C стандардот XML Енкрипција (XML Encryption Syntax and Processing, W3C Recommendation) обезбедува XML шема и множество од процесирачки правила кои поддржуваат енкрипција/декрипција од цели документи, вклучувајќи XML документи, XML елементи и содржина од XML елементи.

Заедно со XML Потпис, XML Енкрипција е основач на повеќе прифатени стандарди, во индустријата за безбедна размена на XML базирани документи (Web Services Security, SAML, ISIS MTT, ebXML-Messaging, FinTS, OSCI-Transport).

7 Структура на документите и податоците што се разменуваат

Евидентирањето на структурата на документот во базата на комуникацискиот сервер започнува со поднесување на барање во кое е опишана структурата на документот кој се евидентира во електронска форма од страна на органот.

Структурирани документи се документи во XML формат чија структура е евидентирана во базата на податоци на комуникацискиот сервер. Структурата на XML документите што се пренесуваат преку Единствената околина се опишува преку XML шема. Xml шема јазикот се референцира како XML Schema Definition (XSD). Целта на XML шема е да ги дефинира легалните градбени блокови на еден XML документ. XSD (XML Schema Definition) може да се користи да изрази множество од правила кои што XML документот треба да ги усогласи според таа шема со цел да се смета за "валиден". XML шема е W3C препорака.

XML шема:
-дефинира елементи кои можат да се појават во документ,
-дефинира атрибути кои можат да се појават во документ,
-дефинира кои елементи се деца елементи,
-дефинира поредокот на деца елементите,
-дефинира бројот на елементите деца,
-дефинира дали елемент е празен или може да вклучи текст,
-дефинира податочни типови на елементи и атрибути,
-дефинира подразбирливи и фиксни вредности за елементи и атрибути.

Секој XML документ што е предмет на размена а произлегува од одредена институција е неопходно претдходно од страна на институцијата што го издава, да изготви структурата на XML документот т.е XML шема и истата да биде доставена до секторот за интероперабилност во МИОА, Министерството потоа ја евидентира структурата, и дава согласност за размена на XML документи кои се валидни во однос на таа шема.

Доколку се јави потреба од размена на неструктуирана документи, истите се пренесуваат во рамки на содржината на структуриран документ.

8 Планирање на основни елементи на архитектура за комуникација со системот за Интероперабилност

За комуникација со системот за интероперабилност, потребна е поткрепа од следниве стандарди:

- TCP/IP за начин на транспорт;
- HTTPS за обезбедување на шифрирана комуникација;
- HTML, XHTML и XSL за презентација на информациите базирани на веб-страници;
- XML за структуриран и конзистентен начин на размена на информациите;

- x.509 сертификати – кога се бараат дигиталните сертфикати и дигиталните потписи;
- W3C стандардите за дигитални потписи и PKCS како методи за употреба на дигиталните сертификати за дигитално потпишана информација;
- SOAP за пристап до системите независно од производителите;
- SMTP и SMIME/3 за размена на e-mail;
- Веб сервиси како примарни методи независни од производителот кои комуницираат со други сервиси.

При планирањето на системската архитектура, треба да се земат во предвид следниве точки, со цел да се олесни семантичката интероперабилност:

- За размена на податоци, се употребува XML формат со https протокол;
- XML форматот кој се употребува треба да биде лесен за разбирање и да не содржи непотребни тагови и детали;
- XML форматот кој се употребува треба да биде документиран за да биде лесно разбирлив за развивачите на софтвер;
- конвенции за номенклатура (именување) и верзионирање би го намалил трошокот за менаџирање на (XML) шемите и би ја намалил веројатноста за нивна повеќекратна употреба.

8.1 СОА и Веб сервиси

Крајните точки на услугата кои се достапни во сервисно ориентираната архитектура, користат Веб сервиси, кои пак се изградени од следниве стандарди:

- XML: eXtensible Markup Language, кој овозможува податочна интероперабилност помеѓу системите, независно од производителите;
- SOAP: Simple Object Access Protocol, кој ја овозможува синтаксата за пристап до услугите (сервисите);
- WSDL: Web Services Description Language, кој ефективно ги задоволува потребите на веб сервисите и ги регулира влезни параметри за да се овозможат бараните излезни параметри.

8.2 Размена на пораки

Размената на пораки во системот е исто така една од основните компоненти за успешна интероперабилност. Постојат стандарди за Web сервиси кои вклучуваат:

- SOAP 1.1: основен распространет стандард за размена на пораки преку различни транспортни протоколи, вклучувајќи го и HTTP;
- SOAP 1.2: поправена верзија на основниот стандард;

- UPNP (abbr. Universal Plug and Play) Верзија 2 Протокол за Приказ на Веб сервиси: Проткол кој е интегриран во UPNP v2 архитектурата;
- WS-Addressing: обезбедува транспортно неутрални механизми за адресирање на Веб Сервиси и пораки;

Паралелно со барањата за пораките се и потребите кои вклучуваат предвидливост и сигурност. Постои комплет на спецификации за Web сервиси кои што се одредени за да обезбедат сигурност и тие вклучуваат:

- WS-ReliableMessaging: протокол за размена на пораки кој праќа SOAP пораки во двонасочна комуникација помеѓу две крајни точки;
- WS-TransmissionControl: комплет на конструкции за контролирање на размената на пораки помеѓу сервиси , со цел да се подобри сигурноста, при загуба на пораки за време на недостапност на сервисот;
- WS-EndpointResolution: комплет на Веб Сервис механизми кои овозможуваат избор на специфична крајна точка на комуникација од листа на слободни кандидати.

За вршење на заштитена размена на пораки по протоколите HTTP, LDAP, FTP и други да се користи протоколот SSL ("Secure Socket Layer - Слој на сигурното соединување") верзија 3.0 и сл., основан на Препорака RFC 2246, усвоена од IETF (The Internet Engineering Task Force - Целна група за интернет инженеринг) преку јануари 1999 г. или VPN ("Virtual Private Networking - Виртуални приватни мрежи") - решенија за сигурно криптирање на сесиите, основан на Препорака RFC 4026, усвоена од IETF (The Internet Engineering Task Force – целна група за интернет инженеринг) преку март 2005 г.
Како алтернатива на SSL v3, може да се користи и Transport Layer Security (TLS) верзија 1.0 и следни верзии.

За потребите на користење на електронски административни услуги се допушта примањето на следните затворени фајлови формати на електронски документи со неструктурирана содржина:

- фајлови формати, кои имаат можност да вклучат во себе си електронски потпис:
  - "pdf" (Adobe Portable Document Format, создаден од компанијата Adobe);
  - "doc" (Document Format, создаден од компанијата Microsoft);
  - "docx" (Document Format, создаден од компанијата Microsoft);
  - "xls" (Excel Sheet Format, создаден од компанијата Microsoft);
  - "eml" (EML Format за електронска пошта, создаден од компанијата Microsoft)
  - "odf" (ISO/IEC 26300:2006 – OpenDocumentFormat), и
  - др.

- фајлови формати, кои немаат можност да вклучат во себе си електронски потпис:
  - стандардизиран формат "p7s" (по стандард PKCS#7 (Public Key Cryptography Standard - Стандард за криптографија на јавниј клуч) на RSA Data Security, усвоен со Препорака RFC 2315 на IETF (The Internet Engineering Task Force - Целна група за Интернет инженеринг) од март 1998 г., кој капсулира електронските документи и одделниот електронски потпис ("detached signature");
  - формат "ats", кој капсулира електронските документи, одделниот електронски потпис, како и други уточенија ("time-stamp tokens", "certificate status" и др.).

- фајлови формати, потпишани и сврзани со електронски потпис преку "PKCS#7" и "ATS" со вклучено содржина на фајлот:

  - "sxw" (создадени со средствата на Open Office);
  - "txt" (текстуални фајлови во ASCII 7-битов формат, unicode формат, кодиран во 8-битско UTF-8 или CP1251 претставување);
  - "rtf" (Rich Text Format v1.6, v1.7, v1.8 и сл. текстуални фајлови);
  - "jpg", "jpeg" (JPEG JFIF v1.02 и сл. растерни графички фајлови);
  - "j2k", "jpx", "jp2" (JPEG 2000, JP2 или JPX растерни графички фајлови);
  - "png" (PNG v1.2 и сл. растерни графички фајлови);
  - "tiff" (TIFF rev. 6.0 и сл. растерни графички фајлови).

Административните органи, лицата, кои вршат јавни функции, и организациите, кои доставуваат јавни услуги, се должни:

- Да користат информатички системи, кои отчитуваат астрономско време по стандард UTC (Coordinated Universal Time), базиран на Препорака 460-4 "Standard Frequency and Time Signal Emissions - Стандардна фреквенција и давање на временски сигнал" од 1986 г. на Меѓународниот сојуз по телекомуникации (ITU - International Telecommunications Union).
- Времето се отчитува по националната часовна зона Средно европско време (UTC+1) .