Жүйе электронды құжат айналымы (EDO)

**Кіріспе**

## Жүйе EDI

EDI - Бұл жүйесі берілістер электрондық құжаттар, В біріктірілген :

* білдіреді криптографиялық қорғау ақпарат;
* жүйесі басқару ашық пернелер.

Жүйе EDI пайдаланылады үшін берілістер ақпарат арасында қолданбалар Бірыңғай сауда жүйесінің есеп айырысу инфрақұрылымының саудасы .

## Сипаттама құжат

Нағыз құжат арналған үшін потенциал пайдаланушылар ETS электрондық құжат айналымы жүйелері.

Мақсат құжат - беру жалпы өнімділік туралы сәулет, жұмыс істеу принциптері және ақпаратты өңдеу жүйелерінде электрондық құжат айналымын пайдалану мүмкіндіктері.

# Жалпы интеллект

## Сипаттама жүйелер

Соңғы пайдаланушының көзқарасы бойынша EDI жүйесі кірістірілген криптографиялық құралдары бар мамандандырылған электрондық пошта болып табылады. қорғау ақпарат Және басқару ашық пернелер.

Берілетін ақпаратты ашудан және жалғандықтан қорғау үшін EDI жүйесі пайдаланады сертификатталған бағдарламалық қамтамасыз ету қауіпсіздік шифрлау Және электрондық цифрлық қолтаңба (ЭСҚ).

Клиент-Банк немесе Клиент-Депозитарий типті жүйелерде қолданылатын көптеген хабарламаларды жіберу ішкі жүйелерінен EDI-ның айрықша ерекшелігі - бұл алмасу хабарлар Авторы принципі «әрбір бірге «барлығы». Бұл қатысушылар арасындағы шарттық қатынастар жүйесімен, сондай-ақ қолданылатын жүйемен қамтамасыз етіледі

тарату ашық пернелер жазылушылар Және өңдеу ақпарат О қорытынды олардың әрекетінен .

## Пайдаланушылар EDI

Жүйе EDI қамтамасыз етеді мүмкіндік алмасу қаржылық құжаттар арасында Биржаның есеп айырысу инфрақұрылымының барлық қатысушылары мен субъектілері.

## Артықшылықтары электронды құжаттар

Қазіргі заманғы деңгейі дамыту телекоммуникациялар технологиялар жасайды Мәселе азайған жағдайда электронды құжаттарды пайдалану сөзсіз

шығындар Және төмендеуі тәуекелдер сағ алмасу заңды түрде маңызды ақпарат. EDI пайдалану келесі шығындарды азайтуға мүмкіндік береді :

* дайындық шығыс құжаттары;
* берілу құжаттар;
* енгізу, тексеру және өңдеу кіріс құжаттар.

EDI-де ақпарат алмасу жылдамдығы құжаттардың ішкі тасымалдануына байланысты емес бір ғимараттар немесе арасында әртүрлі аймақтар елдер. Қысқарту уақыт өңдеуге байланысты транзакцияны орындау цикліндегі технологиялық операциялар үшін

құжаттар, мүмкіндік береді жылдамдату процесс қорытындылар Және есептеу транзакциялар, азайту шығындар.

Қорғалған электрондық қолтаңба беріліп жатқан құжаттар орнатуға мүмкіндік береді авторлық электронды құжат. қоспағанда Того, жоқ түзетулер Жоқ қол қойылған құжатқа оның электрондық цифрлық қолтаңбасының тұтастығын бұзбай енгізілуі мүмкін.

Қарапайымдылық тексереді ЭСҚ Және мүмкін емес оның контрафактілік мүмкіндік береді болдырмау тәуекел құжаттарды қолдан жасау. Жаңа абоненттердің ашық кілттерін тарату жылдамдығы және оларды пайдалану аяқталғаннан кейін кілттерді қайтарып алу жылдамдығы криптографиялық кілттерді рұқсатсыз пайдалану қаупін айтарлықтай төмендетеді. Шифрлау алгоритмдері мен электрондық қолтаңбалардың сенімділігі олардың көп жылдар бойы тексерілген

пайдалану В әртүрлі банк ісі жүйелер, В көлемі саны В Ұлттық Қазақстан Республикасының Банкі .

## Заңды күш ЭСҚ

Сәйкес заңнама ҚР, құжаттар В электронды пішін, дәл Сонымен бірдей Қалай ал қағаздағы құжаттар қарапайым жазбаша түрде жасалған болып есептеледі.

үшін формациялар ЭСҚ Және шифрлау хабарлар EDI пайдаланады бағдарламалық қамтамасыз ету

қауіпсіздік криптографиялық қорғау ақпарат Тұмар CSP сертификатталған республикада Қазақстан қосулы хат алмасу талаптар қауіпсіздік, құрылды " ҚР СТ 1073 – 2007".

Дұрыс пайдалану қорлар қорғау ақпарат қамтамасыз етілген ақпараттық технологиялар бойынша ETS-пен келісімге қол қойған EDI жүйесінің пайдаланушылары

қызмет көрсету. Пайдаланушылар бойынша EDI алады болу Және күй ұйымдар, және олармен шарттық міндеттемелермен байланысты коммерциялық кәсіпорындар.

## Қажеттілік байланыстар EDI -ге

Бастау қанау жүйелер EDI болып табылады маңызды кезең В дамыту ETS Қалай жаңа технологияларды енгізудің негізі ретінде сауда - есеп айырысу жүйесі құрылды:

* Орталық электронды келісім-шарттар;
* Есептер Авторы схема «жабдықтау қарсы төлем»;
* Сауда бірге алдын ала депозитке салу.

Қолданылуы жүйелер EDI мүмкіндік береді бас тарту бастап пайдалану қағаз

құжаттар сағ жасау транзакциялар сатып алу және сату тауарлар, оның ішінде дизайн мәмілелер және жасалған мәмілелер бойынша есеп айырысулар.

EDI-ге қосылу нарық қатысушыларына бір жүйені пайдалану мүмкіндігін береді үшін алмасу құжаттар бірге барлығы бойынша ұйымдар, жүзеге асыру ETS биржасында сауда жасау және онымен есеп айырысу ETS клирингтік орталығы.

# Техникалық сипаттамасы

## Негізгі ұғымдар криптография

үшін қорғау ақпарат сағ аудару Авторы телекоммуникациялар арналар EDI сертификатталған Tumar CSP бағдарламалық өнімінде жүзеге асырылған криптографиялық түрлендіру алгоритмдерін пайдаланады .

Криптографиялық түрлендірулердің жұмысы криптографияны қолдануға негізделген пернелер - жинақтар деректер, бірегей арқылы қалыптасады жол қосулы сандардың кездейсоқ тізбегіне негізделген. Алгоритмдердің екі негізгі түрі бар

шифрлау – симметриялық және асимметриялық. Симметриялық шифрлау алгоритмін қолданғанда жіберуші және алушы да оны пайдалануы керек шифрлау және шифрды шешу үшін бірдей криптографиялық кілт және жіберу мәселесі бар бұл кілт арасында екі жазылушылар. Асимметриялық алгоритм екеуін пайдаланады кілт - бір үшін шифрлау, А басқа үшін шифрды шешу . Бір бастап бұл кілттер

сайын пайдаланушы міндетті сақтау В құпия (бұл кілт деп аталады құпия), А басқа кілт кіммен хабарлама алмасқысы келетінін хабарлайды (ашық кілт).

Егер асимметриялық алгоритм арқылы шифрлау үшін ашық кілт пайдаланылса, Бұл үшін шифрды шешу - сәйкес құпия кілт Және қарама-қарсы. Ашық және жабық кілттер арнайы математикалық қатынас арқылы байланыстырылған, ол ашық кілттің сәйкеске тиесілі екенін тексеруге мүмкіндік береді.

құпия кілт, Бірақ Жоқ мүмкіндік береді есептеу мағынасы құпия кілт мағынасы бойынша

ашық. Артықшылық асимметриялық алгоритм В көлемі, Не Ол мүмкіндік береді ашық кілттерді байланыс арналары арқылы жіберу, бірақ, екінші жағынан, алгоритмнің күрделілігіне байланысты

жылдамдық жұмыс істейді бағдарламалар қосулы оның негізі айтарлықтай төменде, Қалай бағдарламалар қосулы симметриялық алгоритмге негізделген.

үшін шифрлау В бағдарламалық қамтамасыз ету өнім СКЗИ Тұмар CSP пайдаланылады симметриялық схема алгоритм шифрлау бірге ашық тарату кілттер, Не

мүмкіндік береді біріктіру жылдамдық жұмыс істейді симметриялы алгоритм Және ыңғайлылық кілтті бөлу. Электрондық құжатты шифрлау үшін жіберуші пайдаланады

туынды кілт, қай шығады бірге көмегімен математикалық жіберушінің құпия кілтін және алушының ашық кілтін түрлендіру. Хабарламаның шифрын шешу үшін алушы өзі алатын туынды кілтті пайдаланады

көмегімен өзінің құпия кілт Және ашық кілт жіберуші. үшін әрқайсысы Жіберуші мен алушы жұптары үшін туынды кілт бірегей болады.

ЭЦҚ жұмыс істеу принципі асимметриялық шифрлау алгоритміне негізделген. Электрондық цифрлық қолтаңба – жүйелілік деректер, қалыптасуда бастап жіберілді электронды хабарлар бірге

жіберушінің құпия кілті арқылы арнайы шифрлау алгоритмін қолдану Және жіберілді бірге бірге бұл хабар. Тексеру ЭСҚ Мүмкін құжатқа қол қойған пайдаланушының ашық кілті бар кез келген абонент. ЭЦҚ-ның ашық кілті «қолтаңба картасының» аналогының бір түрі ретінде әрекет етеді .

Криптографиялық алгоритмдердің «бұзуға» (құпия кілтті таңдау) төзімділігі анықталады. математикалық қасиеттері пайдаланылады функциялары. Ұзындығы кілт Бұл санау арқылы оны іздеу үшін бар қуатты компьютерде жүздеген жылдар қажет болады .

## Архитектура EDI

Құрылымдық жағынан жүйесі тұрады бастап Орталық EDI, орналасқан қосулы қор биржасы ERTS Және пошта серверлері - EDI абоненттерінің жергілікті желілерінде орнатылған пошта жәшіктері .

IN функциялары Орталық EDI кіреді сақтау сертификаттар ашық кілттер, чектер

шындық сертификаттар барлығы өту арқылы ол хабарлар Және кепілдіктер олардың электрондық цифрлық қолтаңбаны пайдалану (кілттерді басқару туралы қосымша ақпарат алу үшін 3.3. бөлімін қараңыз), сондай-ақ жүйе уақытын сақтау.

Пошта жәшігі хабарламаларды басқа абоненттердің пошта жәшіктеріне жіберу функцияларын орындайды , өзара әрекеттеседі. бірге Орталық EDI Және қолданбалар финал пайдаланушылар. Бір пошта жәшігінен екіншісіне хабарлар EDI орталығында аралық сақтаусыз тікелей жіберіледі (толығырақ ақпаратты 0-б. қараңыз).

Қолданбалар қосылып жатыр Кімге EDI арқылы Пошта жәшігі . TO жалғыз Пошта жәшігі Мүмкін қолданбалардың кез келген санын қосуға болады.

Өзара әрекеттесу қолданбалар Және пошта серверлер болып жатыр Авторы хаттама,

динамикалық болып табылатын қолданбалы бағдарламалау интерфейсінде (API) жүзеге асырылады жүктеп алуға болады кітапхана Windows ( dll ). Егер қиындықтар dll Жоқ алады болу

кіріктірілген В өтініш, Бұл мүмкін пайдалану интерфейс алмасу файлдық шлюз арқылы файлдық жүйе арқылы хабарлар.

## Хабарды жіберу

Сағат қабылдау хабарламалар, Пошта жәшігі алушы ақпаратты растауды автоматты түрде жасайды және EDI орталығы арқылы жіберушіге жібереді

жеткізу құжат. Растау жеткізулер қамтиды ЭСҚ Пошта жәшігі алушы және EDI орталығымен куәландырылады және қажет болған жағдайда жіберушіге хабарламаның жеткізілгенін дәлелдеуге мүмкіндік береді. Жіберушінің пошта жәшігі бұл хабарламаны алғанға дейін хабарлама жеткізілді деп саналмайды және белгілі бір аралықтан кейін

уақыт әрекет кетулер қайталайды. Бұл сияқты жол жүзеге асырылуда кепілдендірілген жеткізу, яғни жіберуші жеткізілім туралы хабарлама алғанша хабарламаны жіберіледі деп есептемейді.

## Бақылау пернелер

Абоненттің сертификаттау орталығымен жұмыс істей бастауы үшін бастапқы инициализациялау кілттері, В көлемі саны үшін олардың ауыстырулар қосулы криптографиялық пернелер электронды электрондық цифрлық қолтаңбаны ETS алмасу менеджері немесе абонент дербес жасай алады.

Таралу ақпарат туралы ашық пернелер қолдар Және шифрлау абоненттер сертификат механизмі арқылы жүзеге асырылады. EDI-ге қосылу сатысында

ұйымдар CA-дағы бастапқы инициализациялау кілттерін криптографиялық кілттермен ауыстырады ЭСҚ Және хабарлайды туралы бұл қор биржасы, Егер жазылушы өз бетінше жасайды пернелер Ол ETS-ті ашық кілт туралы ақпаратпен қамтамасыз етеді, оның негізінде ETS осы кілттің электрондық сертификатын жасайды және оны EDI орталығының деректер қорына орналастырады.

Бағдарламалық қамтамасыз ету қауіпсіздік Пошта жәшігі немесе қолданбалар сұраныс жібереді қосулы сертификат EDI орталығына кез келген абоненттің ашық кілті туралы ақпаратты алу қажет болған сайын. EDI орталығына сұраныстардың санын азайту үшін алынған сертификаттар Пошта жәшігі мен қолданбаның жергілікті дерекқорында сақталады .

Егер ұйымдар қажет қайтарып алу менікі кілт бастап өтініштер, Бұл ол бағыттайды В Ашық кілтті кері қайтарып алуға арналған ETC қағаз құжаты немесе [https://ca.kisc.kz/ CA](https://ca.kisc.kz/) веб- порталы арқылы оны қайтарып алады .

Барлығы хабарламалар, өту арқылы Орталық EDI, тексерілуде қосулы Бұл, Не сертификаттар осы хабарламада пайдаланылған барлық ашық кілттер жарамды, содан кейін

хабар сертификатталған ЭСҚ Орталық EDI бірге көрсеткіш уақыт хабарлама жіберу .

Қол қою Орталық EDI астында хабар білдіреді, Не Барлығы сертификаттар, көрсетілген В

тақырып хабарлар болды жарамды қосулы сәт өту бұл хабарлар EDI орталығы арқылы.

## Артықшылықтары

Авторы салыстыру бірге басқалар жүйелер қорғалған берілістер электронды хабарлар EDI техникалық сипаттамаларының бірегей жиынтығына ие:

* жоғары дәрежесі қауіпсіздік;
* мүмкін емес пайдалану алынып тасталды бастап әрекеттер пернелер кейін Того, жүйеде кілтті алу фактісі қалай тіркеледі;
* қолжетімділігі дамыған жүйелер басқару ашық кілттер, мүмкіндік беру

өзара әрекеттесу арасында пайдаланушылар арқылы жүйелер Авторы принципі «әрбір әрқайсысымен »;

* тарату хабарлар онсыз аралық сақтау В орталық;
* «технологиялық» В қанау Және техникалық қызмет көрсету;
* ашық API үшін интеграциялар қолданбалар бірге жүйесі EDI.

## Техникалық талаптар

Net электронды құжат айналымы E TS салынып жатыр бірге пайдалану сол бірдей байланыс арналары, қай пайдаланылады үшін байланыстар Жұмысшылар станциялар ETS. Барлығы, Не ETS қатысушысына EDI-ге қосылу үшін Windows жүйесі бар дербес компьютер қажет.

NT/2000 Және қосылған Кімге сегмент желілер, бар шығу В ETS, Мысалы, Кімге соған ETS жұмыс станциялары орнатылған сегмент. Интернет арналары арқылы қосылуға болады.

Пошта сервер Мүмкін орнатылады қосулы бір ДК бірге Жұмыс істеу станциясы немесе

Орташа сервер ETS. Қолданба EDI, өзара әрекеттесу бірге Пошта жәшігі онымен бір компьютерде де жұмыс істей алады.

ETS үшін ақпараттық технологияларды қолдау қызметтерін ұсыну шарттары EDI Қатысушы орындауы тиіс ақпараттық қауіпсіздік талаптарын белгілейді. Осы талаптарды орындау Қатысушының жауапкершілігінде. Талаптар анықтайды қажеттілік орындау ұйымдастырушылық Және техникалық шаралар Авторы қорғау

құпия пернелер Және бағдарламалық қамтамасыз ету қамтамасыз ету бастап рұқсатсыз пайдалану.