

ПРИМЕР РЕАЛИЗАЦИЈЕ ЕЛЕКТРОНСКОГ ФИНАНСИЈСКОГ ПОСЛОВАЊА

Небојша Радојевић, Зорица Лазаревић, Сениша Ранков, Народна банка Југославије – Београд
 Мирјана Зафировић-Вукотић, Институт "Михајло Пупин" - Београд

Садржај – У овом раду су укратко описани: S.W.I.F.T. мрежа, коришћено телекомуникационо окружење за повезивање Народне банке Југославије са њом и методе шифровања порука које се преносе између корисника и мреже.

1. УВОД

S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunication) је водећа организација у свету за безбедносне финансијске комуникације. У њега је тренутно укључено преко 6000 финансијских институција из 164 земље. Оне су у 1997 год. међусобно разменили преко 800 милиона порука.

2. ОПИС СИСТЕМА [1]

Да би омогућио приступ својим сервисима, S.W.I.F.T. корисницима ставља на располагање глобалну телекомуникациону мрежу, S.W.I.F.T. преносну мрежу – STN (S.W.I.F.T. Transport Network). Логичка архитектура STN-а је у складу са правилима која је ISO прописао за OSI референтни модел. Самим тим дозвољено је логичко раздвајање између, на пример, протокола за линијско повезивање, процедура приступа систему, процедура управљања системом, имплементације индивидуалних сервиса, ...

Приступна тачка у STN се назива SAP (S.W.I.F.T. Access Point). То је физички безбедно место које је нон-стоп контролисано и надзирано од стране оперативног центра S.W.I.F.T.-а. У сваком SAP-у се налази један или више мрежних чворова. Један корисник се преко једног мрежног чвора, тј. преко његовог улаза, повезује на STN. SAP такође обезбеђује физичко повезивање са другим чворовима у мрежи. Главни задатак сваке приступне тачке је да прима и прослеђује поруке од и ка корисницима користећи најфикаснији пут кроз STN. Ако тачка приступа откаже све сесије тренутно прикључених корисника на њу биће прекинуте. Да би наставили са радом они морају успоставити везу са неким другим SAP-ом.

При повезивању на S.W.I.F.T. потребно је користити X.25 пакетско-комутирани протокол. Овим се, поред осталог, омогућава корисницима да преко исте линије приступају различитим сервисима.

Кроз STN корисници тренутно могу приступити следећим S.W.I.F.T. апликативним сервисима:

- FIN (Store-and-forward Message Transfer). Он омогућава финансијским институцијама да размењују структуриране финансијске податке, безбедно, брзо и поуздано по целом свету.
- IFT (Interbank File Transfer). Овај сервис се користи при преносу велике количине података и он може да прихвати информације у било ком формату договореном између кореспондената.
- INT (Interactive). Служи за допуну претходна два сервиса. INT обезбеђује, у реалном времену, интерактивно повезивање преко STN-а, на пример: финансијских сервиса и одговарајућих сервиса понуђених од S.W.I.F.T.-а или неког другог провајдера. INT није расположив као генерички мрежни сервис већ је он компонента пакетске сервисне понуде.

У погледу безбедности и брзине најстроже захтеве поставља FIN сервис. У оквиру сваког апликативног сервиса у општем случају дефинисано је више различитих типова порука

Сваки покушај успостављања везе са S.W.I.F.T. апликативним сервисом, који стигне на улаз, се прво рутира ка ван-мрежном NWD (Network Directory) сервису. Овај сервис се само користи у току успостављања везе. Главна функција NWD-а је да провери исправност садржаја тражене везе, који обухвата комбинацију симболичке адресе и захтеваног сервиса, упоређујући га са садржајем своје сопствене базе података. Ако је све у реду успоставиће се веза са одговарајућим сервисом.

За приступ било ком S.W.I.F.T. сервису корисник мора имати:

- Симболичку (идентификациону) адресу
- Одговарајући апликативни софтвер инсталиран на серверу и радним станицама
- Комуникациону линију до тачке приступа у STN

У синтакси симболичке адресе разликујемо три целине:

- дестинацију (одређиште), дефинисану са 8 карактера
- идентификацију повезивања, дефинисану са 2 цифре
- поддестинацију (опционално), дефинисану са 3 цифре

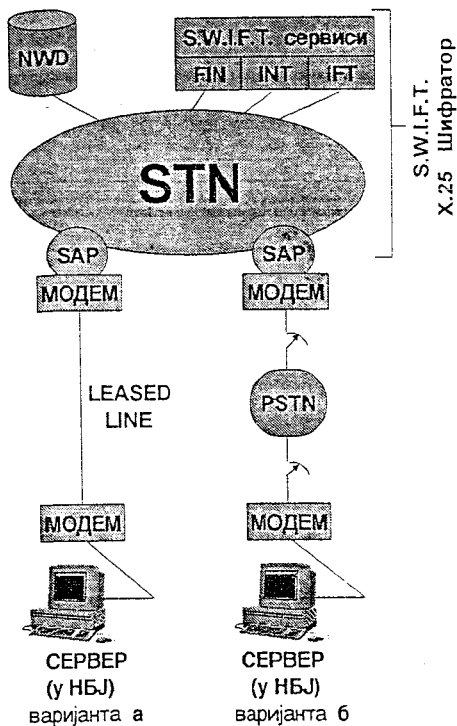
Симболичка адреса НБЈ (Народне банке Југославије) је NBYUYUBG01000.

У НБЈ сервер је под оперативним системом AIX. На њему је инсталиран SWIFT Alliance Access

софтвер. Радне станице су под оперативним системом Windows NT 4.0 Workstation. На њима је инсталиран SWIFTAlliance Access Workstation софтвер. Сервер и радне станице су преко TCP/IP протокола повезане у LAN мрежу која је тренутно потпуно затвореног типа.

У НБЈ се користи два типа комуникационих линија:

- Изнајмљена (Leased), приказана на сл. 1 (варијанта а)
- Комутирана (PSTN, тј. "Dial-up"), приказана на сл. 1 (варијанта б)



Сл. 1 Типови комуникационих линија

Изнајмљена линија

S.W.I.F.T. подржава два типа аналогних изнајмљених линија:

- 2-жична од тачке до тачке
- 4-жична од тачке до тачке.

Максимално подржана брзина приступа је 9.6Kbps. Препоручени квалитет линије треба да задовољи ITU-T M.1040 препоруку за брзину од 2.4Kbps и ITU-M.1020 за брзину већу од 2.4Kbps.

Ако корисник има више изнајмљених линија оне ће све бити рутиране у исту приступну тачку.

Пожељно је да модем који се користи поред стандардни функција (предаје и пријема података, успостављања и одржавања комуникационе везе, конвертовања дигиталних података у аналогне и обрнуто, аутоматског бирања тел. бројева, ...) поседује и DBR (Dial Back Restoral) функцију. Она омогућава да се реконструише веза преко комутиране у случају отказа изнајмљене линије. Без обзира што модеми могу бити међусобно компатибилни S.W.I.F.T. препоручује да се на истој линији не користе различити типови. Модем који се користи за изнајмљену линију мора да задовољи један од следећих стандарда:

- V.22 bis (2-жична веза, DBR дозвољен)
- V.26 (4-жична веза)
- V.27 (4-жична веза)
- V.29 (4-жична веза)
- V.32 (2-жична или 4-жична веза, DBR дозвољен)
- V.32 bis (2-жична или 4-жична веза, DBR дозвољен)
- V.33 (4-жична веза, DBR дозвољен)
- V.34 (4-жична веза, DBR дозвољен)

Дигитална изнајмљена линија, где је то могуће, може да се користи.

Једина тачка приступа у STN у Југославији се налази у ТК центру (у Катифевој улици) Телекома Србије. НБЈ до ње користи аналогу 4-жичну изнајмљену линију са брзином приступа од 9.6Kbps.

Комутирана линија

S.W.I.F.T. преко комутиране линије подржава два типа повезивања:

- Резервисано. Ово је слично коришћењу изнајмљене линије. Овде је један улаз у STN резервисан за одређеног корисника. Недостатак је што се у случају отказа додељеног улаза није могуће пребацити на други.
- Дељено. Ово је најједноставније и најчешће се користи и само ћемо њега даље посматрати.

Комутирана веза се успоставља бирањем. Ако у приступној тачки (коју смо позвали) постоји слободан улаз у STN он се додељује кориснику, у противном добија се сигнал заузећа. Корисник може приступити S.W.I.F.T. мрежи кроз било који SAP у било ком делу света.

Као и код изнајмљене линије и овде је максимално подржана брзина приступа 9.6Kbps.

Коришћени модем за комутирану линију мора да задовољи један од следећих стандарда:

- V.22 bis
- V.32
- V.32 bis
- V.34

НБЈ комутирану линију користи само у случају отказа изнајмљене. Веза се првенствено успоставља са нашом приступном тачком у STN. У случају неуспеха врши се успостављање везе са неким другим SAP-ом.

Пре слања одређени, битни делови поруке се обавезно шифрују тајним кључем пошиљаоца и јавним кључем примаоца. S.W.I.F.T. шифрује (X.25 шифровањем) целокупан саобраћај који се преноси преко STN-а. Саобраћај на линији између корисника и SAP-а није шифрован. Корисник на том делу, као што је приказано на сл. 2, може извршити шифровање садржаја комплетне поруке и то:

- линијским шифровањем
- X.25 шифровањем

Код линијског шифровања се цела порука, укључујући оквир и контролне податке шифрује. Овим се обезбеђују подаци, а анализа саобраћаја услед континуалног шифровања није могућа. STN захтева да подаци на њеним улазима буду у сагласности са X.25 протоколом. Због тога порука која је била линијски шифрована мора на SAP-у прво да се дешифрује па тек после тога да се шаље кроз STN. Ово је главни недостатак ове методе.

X.25 протокол као што знамо раставља поруку у блокове, тј. пакете, који се у општем случају састоје од: карактера синхронизације, хедера, дела података и трејлера. Код X.25 шифровања врши се само шифровање дела података у пакету. Заглавље и трејлер се не шифрују. Овим се обезбеђује да се подаци правилно рутирају кроз STN. Главна предност X.25 шифровања података је да саобраћај између корисника и S.W.I.F.T. централе никада није чист. Подаци се само једном, одмах при слању, шифрују на страни корисника и први пут дешифрују тек на пријему, приликом обраде у S.W.I.F.T.-у. Због овога S.W.I.F.T. препоручује да се користи X.25 шифровање.

У НБЈ се засада не користи ни једна од ове две методе шифровања.

3. ЗАКЉУЧАК

С' обзиром на то како је тренутно остварена веза између НБЈ и S.W.I.F.T.-а цео систем обезбеђује потребан ниво поузданости, безбедности и брзине рада. Али ако би се, на пример, извршило повезивање преко јавне мреже за пренос података (PDN-Public Data Network) обавезно би се пре слања морало урадити X.25 шифровање поруке.

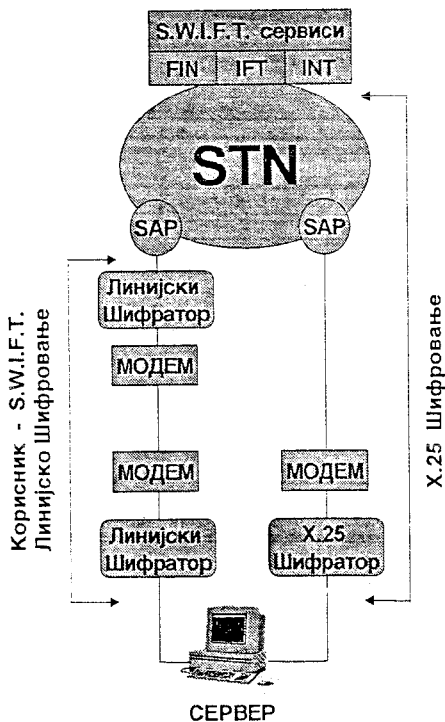
ЛИТЕРАТУРА

[1] Оригинална S.W.I.F.T. документација

Abstract – This paper brings description of the: S.W.I.F.T. network, the telecommunication surroundings applied in connection the National Bank of Yugoslavia with the S.W.I.F.T. as well as the methods of encrypting messages transmitted between user and network.

EXAMPLE OF ELECTRONICALLY OPERATED BUSINESS TRANSACTIONS

Nebojsa Radojevic, Zorica Lazarevic, Sinisa Rankov, Mirjana Zafirovic-Vukotic



Сл. 2 Методе шифровања