

Komunikacja z systemem Edinet

Wymiana dokumentów między partnerami biznesowymi (B2B - Business to business), w której bardzo istotna jest niezawodność i bezpieczeństwo do niedawna była realizowana przeważnie za pomocą standardu EDI i poczty X400.

Niestety koszt przepływu danych przez sieć dzierżawioną jest wysoki. Wiele firm chcąc zredukować koszty zdecydowało się na alternatywne metody wymiany danych, charakteryzujące się przepływem danych przez ogólnie dostępne łącza internetowe i zastosowaniem kryptografii dla zapewnienia bezpieczeństwa. Powstałe w ten sposób metody komunikacji nie pociągają za sobą żadnych kosztów, nie licząc ewentualnych kosztów zastosowanego oprogramowania, lecz są zazwyczaj rozwiązaniami właściwymi dla pary partnerów biznesowych – każda para tworzy własne rozwiązanie.

Chcąc stworzyć jeden standard Internet Engineering Task Force (IETF www.ietf.org) zaprojektowało protokół AS – bezpieczny i wykorzystujący ogólnie dostępne łącza internetowe. Dostępnych jest kilka postaci tego standardu: AS1, AS2 i AS3 z czego najpopularniejszy jest AS2. Przesyłane przez AS2 komunikaty nie muszą być zgodne ze standardami.

Edinet obsługuje większość standardowych komunikatów. Ponieważ nie zawsze standardy zaspakajają potrzeby naszych klientów Edinet obsługuje szereg komunikatów i formatów uzupełniających: <http://www.infinite.pl/pub/doc/fmt/>

1. Metody komunikacji z Edinet

Metoda	Bezpieczeństwo	Koszty	Automa-tyzacja	Opis
SOAP/ webservices	Uwierzytelnianie /autoryzacja, SSL	Brak	Tak	Zgodny ze standardem W3C dostęp do funkcji serwerowych, zapewniający łatwość i swobodę integracji z wewnętrznymi systemami. http://www.edinet.pl/edinet_services/
AS2	Podpis cyfrowy i szyfrowanie	Brak	Tak	Pkt. 6. http://www.infinite.pl/pub/doc/as2-implementation.pdf
FTP	Uwierzytelnianie /autoryzacja, SSL,VPN	Brak	Tak	Patrz pkt. 2. http://www.infinite.pl/pub/doc/komunikacja-FTP.pdf Nasz serwer ftp://ftp.infinite.pl
Poczta X400	Wydzielona dzierżawiona linia	Opłata za dzierżawę zależna od ilości przesył. danych	Tak	Patrz pkt. 5. Skrzynki Polkom400 i IBMX400. Duże bezpieczeństwo, lecz najwyższe koszty. Rozwiązanie to głównie stosujemy z sieciami handlowymi.
Platforma www	Uwierzytelnianie /autoryzacja, SSL	Brak	Nie	Przez platformę www.edinet.pl

2. Używanie FTP do wymiany dokumentów

Protokół FTP służy do transmisji plików. Do transmisji potrzebne są dwie strony: strona pytająca "klient", strona słuchająca i odpowiadająca "serwer" zwykle nasz: <ftp://uzytkownik:haslo@ftp.infinite.pl/katalog/>. Cała transmisja jest widoczna w sieci jako przepływ danych. Przy użyciu SSL dane te są zaszyfrowane, klucz do ich rozszyfrowania wymieniony jest przy inicjowaniu połączenia i znany jest tylko stronom transmisji. Szyfrowanie może zapewnić m.in. program TlsWrap, który uruchomiony na tym samym komputerze działa podobnie jak proxy. TlsWrap jest dostępny zarówno pod platformę Windows jak i Unix doświadczenie wykazuje, że pod Win9x nie działa prawidłowo, ale już pod NT/2000/XP nie ma problemów. Program jest darmowy i można go pobrać ze strony <http://tswrap.sunsite.dk>

Możliwe jest także zapewnienie szyfrowania całego kanału komunikacyjnego, w którym będziemy używać protokołu FTP do wymiany danych. Powstała w ten sposób wirtualna prywatna sieć, wykorzystująca ogólnodostępne łącza internetowe, nazywana jest skrótem VPN.

3. VPN - prywatne kanały transmisji plików

Według definicji, Virtual Private Network VPN jest po prostu rozszerzeniem sieci prywatnej wewnętrznej, na obszar sieci publicznej, która ze swej natury jest mniej bezpieczna. W praktyce, ta sieć publiczna to w większości przypadków Internet. Prywatność w sieci publicznej jest osiągana przy użyciu różnorodnych technik kryptograficznych, takich jak szyfrowanie, autentykacja, autoryzacja oraz podpis elektroniczny. Użycie technik kryptograficznych zapewnia poufność wszelkich przesyłanych danych, zabezpiecza je przed modyfikacją podczas transmisji i gwarantuje, że pochodzą one z właściwego uprawnionego źródła. Zakładając, że nikt niepowołany nie może odczytać ani zmodyfikować przesyłanych informacji, uzyskujemy prywatną sieć rozległą Wide Area Network WAN, która jest w rzeczywistości tunelowana w sieci publicznej.

Zanim opracowano VPN, istniały dwie możliwości połączenia odległych sieci: użycie Internetu lub dedykowanych linii dzierżawionych. Internet jest tani, ale niesie ze sobą ryzyko zewnętrznej ingerencji. Linie dzierżawione są bardziej bezpieczne ale zbyt kosztowne.

Virtual Private Networks to stosunkowo niedroga alternatywa, umożliwiającą budowę dużych sieci prywatnych w oparciu o dostępne sieci publiczne. Za pomocą połączeń VPN dane są przesyłane poprzez istniejącą infrastrukturę telekomunikacyjną, taką jak Internet.

5. X400 – możliwości dostępu

Posiadane skrzynki w Polkom400 i IBM Information Exchange umożliwiają nam wymianę informacji z większością światowych operatorów X400. Umowy międzyoperatorskie z firmami COMARCH, EDISON i XTRADE wzbogacają naszą możliwość komunikacyjne.

TPSA - POLKOM400

Nasz adres: C=pl; A=POLKOM400; O=infinite; S=infinite

Kraj	Operator	ADMD
AT	Plus Communication	ADA, UMI-AT
BE	Belgacom	RTT
DE	Sterling Commerce GmbH kiedys LION Gesellschaft fuer	LION
DE	Deutsche Telekom TELEBOX400	DBP, VIAT
DK	UNISOURCE BUSINESS NETWORKS NEDERLAND B.V.	DK400
FI	Helsinki Telephone Company Ltd.	ELISA

NL	AUCS Communication Services	400NET
NO	POSTNet	TELEMAX
SE	SWEDEN POST	SIL
WW	BT	BT
FI	400NET	EPOSNET
GB	WW BT	RACAL400
AT	AT, UMI-AT	ODE
NO	NO TELEMAX	POST
NO	NO TELEMAX	CONCERT
NO	NL 400NET	400NET
NL	NL 400NET	DCCNET
LU	AT UMI-AT	UMI-LU
GB	WW BT	NHS
GB	WW BT	MARK400, GOLD400, BT
EU	WW BT	BT
DE, DK, CH, BE	UMI-AT uwaga ADMD odpowiadajace odpowiednio krajowi	UMI-DE, UMI-DK, UMI-CH, UMI-BE
AT	UMI-AT	UMI-ADA

GXS.com (było IBM - IBMX400)**Nasze adresy**– **do 16-09-2007:****C=PL; A=IBMX400; P=IEEUR; S=PLINFI; G=PLINFI01****C=PL; A=IBMX400; P=IEEUR; DDA1:IE=PLINFIPLINFI01**– **od 16-09-2007 (zmiana w GXS):****C=PL; A=MARK400; P=IEEUR; S=PLINFI; G=PLINFI01**

Kraj	Operator	ADMD	MTA
FR	Atlas	Atlas	ATLAS
BG	Bank Service	Bs400	BANKMAIL
BE	Belgacom	Rtt	BELGIUM
GB	British Telecomm Gold	Gold 400	BTGLOBALMTA
TH	Comm Authority of Thailand	Cat400	CAT400
IE	Cargo Communities	CCS400	CCSMTA88
CN	China Mail	Chinamailsh	CHINAMAILSH
GB	Cable and Wireless	Cwmail	CWMTA1
DE	DFN	D400	DFNBERLIN2
DE	Deutsche Telekom	VIAT	DTMT-MTA
CZ	EDITEL CZ a.s.	Edivan400	EDIVAN
AE	The Emirates	EMNET	EMNET
SE	Postnet	SIL	EMX
GB	GlobalOne UK	TMAILUK	G1UK-MTA
WW	Sita	SITAMAIL	GMSMTA
FI	Elisa	ELISA	HPY88
SE	Tele2	INTERX	INTERX2
FI	Sonera Corp	MAILNET	MAILNETMTA
AT	Radio Austria	ADA	MHSARA
DK	Danish PTT	DK400	MTA0000
IT	Saritel	MASTER400	MTA5
NL	Unisource	400NET	NET01-NL
PTT	Norway	TELEMAX	NORWAY
GB	Umi-Uk	UMI-UK	PARASOFT

AT	Umi-At	UMI-AT	PLUTO
BE	Seagha	SEAGHA	SEAGHA
SU	Sovmail	SOVMAIL	SOVMAIL
SG	Singapore PTT	STEMS	STEMSMTA
DE	Lion	LION	TANDEM
ZA	South Africa Telecom	TELKOM400	TELKOM400
NO	Norway PTT Telepost	TELEPOST	TPCSE
DE	Xtend	TT	TT-RELAY
IN	Indian PTT	VSNL	VSNL88
IE	Eirtrade and Inet	EIRMAIL400	eirmail2000one
PT	Portugal PTT	MAILPAC	mailpac92
IE	Postgem	POSTGEM	pg400
GB	Racal 400	RACAL400	racal400
SI	Slovenija	MAIL	siol2

6. AS - Applicability Statement

Chcąc stworzyć jeden standard Internet Engineering Task Force (IETF www.ietf.org) zaprojektowało protokół. Dostępnych jest kilka postaci tego standardu:

AS1 - protokół bezpiecznej wymiany danych przez pocztę (SMTP+MIME+podpis cyfrowy obiektu+szyfrowanie obiektu). Wymiana ta przebiega w czasie rzeczywistym (serwis do serwisu), gdy nadawca wysyła list za pomocą serwera SMTP odbiorcy.

Pełna informacja: RFC 3335,
<http://www.ietf.org/rfc/rfc3335.txt>

AS2 - protokół bezpiecznej wymiany danych przez HTTP/S (HTTP/S+MIME+podpis cyfrowy obiektu+szyfrowanie obiektu i sesji). Wymiana ta zawsze przebiega w czasie rzeczywistym (serwis do serwisu).

Pełna informacja: RFC 4130
<http://www.ietf.org/rfc/rfc4130.txt>

AS3 - protokół bezpiecznej wymiany danych przez FTP (FTP+podpis cyfrowy obiektu+szyfrowanie obiektu i sesji). Wymiana ta zawsze przebiega w czasie rzeczywistym (serwis do serwisu)

Pełna informacja: RFC 4823
<http://www.ietf.org/rfc/rfc4823.txt>

Protokół AS2 jest najpopularniejszą implementacją AS, staje się ona główną metodą komunikacji B2B na świecie m.in. dzięki prostocie i małym wymaganiom rozwiązania (komunikacja wykorzystuje jeden port np. 80 lub 443).

Na rynku dostępna jest duża ilość oprogramowania realizującego komunikację przez AS2. Wśród wielu produktów na szczególną uwagę zasługują te, które posiadają certyfikat "drummond-certified as2-product" <http://www.ebusinessready.org/as2.html>. Uzyskanie certyfikatu uwarunkowane jest od poddania produktu testom sponsorowanym przez dwie organizacje: <http://www.uc-council.org/> i <http://www.hcco.us/>.

Implementacje AS2: <http://www.infinite.pl/pub/doc/as2-implementacje.pdf>