Bezpečnostní rozhraní UN/EDIFACT

 (Verze MAKRO 7.9.2001)

Obsah

Bezpečnost EDI systémů - ohrožení, bezpečnostní funkce a mechanismy

Při tvorbě systémů, které mají sloužit k přenosu EDI zpráv, je třeba věnovat zvláštní pozornost bezpečnosti těchto systému a zvláště přenášených dat. Proto je nutné již při projektování systému zvolit vhodnou bezpečnostní politiku, která je potom uplatňována při tvorbě a provozu systému. Základem bezpečnostní politiky je definice možných ohrožení systému, určení odpovídajících bezpečnostních funkcí a jejich účinné implementace pomocí bezpečnostních mechanismů.

Možná ohrožení bezpečnosti pro systém přenosu EDI zpráv lze rozdělit do těchto kategorií:

a) Modifikace zprávy - zpráva je změněna po odeslání oprávněným původcem, buď úmyslně, nebo v důsledku technické chyby.

b) Změna v pořadí zpráv - zpráva může být ztracena během komunikace nebo může být zkopírována a doručena vícekrát, ať úmyslně, nebo v důsledku technické chyby. Pokud je důležité pořadí zpráv, v jakém jsou přijímány, je další možnou hrozbou změna pořadí zpráv.

c) Vydávání se za někoho jiného (Masquarading) - při komunikaci s druhou stranou se účastník systému vydává za jiného oprávněného účastníka.

d) Přístup neoprávněné osoby do systému - osoba, která nemá právo přístupu do systému, se přesto komunikace zúčastní a vydává se za právoplatného účastníka systému.

e) Odmítnutí původu zprávy - původce zprávy později odmítne její odeslání.

f) Odmítnutí příjmu zprávy - osoba, které zpráva byla určena, později odmítne její příjem, přestože jí zpráva byla doručena.

g) Zneužití důvěrné informace - zprávy důvěrného charakteru mohou být získány neoprávněnou osobou nebo jinak zneužity.

Jednou z možností, jak účinně zabránit výše uvedeným ohrožením, je uplatnění následujících bezpečnostních funkcí:

a) Integrita zprávy - tato funkce zaručuje, že modifikace obsahu zprávy během přenosu bude odhalena.

b) Integrita sekvence zpráv - tato funkce zaručuje, že žádná zpráva nebyla zkopírována nepovolanou osobou a odeslána znovu. Umožní také zjistit ztrátu zprávy a změnu v pořadí zpráv.

c) Autentizace zprávy - tato funkce umožňuje určit osobu, která odeslala zprávu.

d) Řízení přístupu - tato funkce umožňuje omezit přístup ke zprávám a komunikaci pouze oprávněným osobám.

e) Neodmítnutí původu zprávy - tato funkce zabezpečuje, že osoba odesílající zprávu, nemůže později popřít odeslání zprávy.

f) Neodmítnutí příjmu zprávy - tato funkce zabezpečuje, že osoba přijímající zprávu, nemůže později popřít přijetí zprávy.

g) Šifrování obsahu zprávy - tato funkce zajišťuje důvěrnost dat během přenosu.

Pro implementaci bezpečnostních funkcí v systému pro přenos standardních zpráv EDI je navržen následující model s bezpečnostními mechanismy, které jsou založeny na účinných kryptografických algoritmech:

Bezpečnostní funkce integrity, autentizace a neodmítnutí původu jsou zajištěny digitálním podpisem zprávy, speciálním kryptografickým algoritmem, založeným na asymetrickém šifrovacím algoritmu.

Pro zajištění neodmítnutí příjmu zprávy může být použito UN/EDIFACT zprávy AUTACK, která jednoznačně potvrzuje příjem určité zprávy, a digitálního podpisu.

Sekvenční integrita je zajištěna pomocí referenčního čísla zprávy, které je sekvenční a unikátní pro každou dvojici uživatelů, a dále pomocí bezpečnostní časové značky. Tak může být při příjmu identifikována duplikovaná zpráva nebo zjištěna ztráta zprávy či změna v pořadí zpráv.

Řízení přístupu může být v aplikacích zajištěno pomocí přístupového hesla, kterým je zabezpečen tajný klíč uživatele, takže nikdo kromě oprávněného vlastníka jej nemůže použít.

Důvěrnost obsahu zprávy je zajištěno enkrypcí zprávy pomocí šifrovacího algoritmu. Pro EDI aplikace je použit symetrický algoritmus DES, který je uznávaným standardem pro šifrování obchodních zpráv.

Bezpečnostní řešení v UN/EDIFACT

V rámci standardu UN/EDIFACT jsou definovány normy, které definují možné způsoby zabezpečení UN/EDIFACT struktur s využitím nejrůznějších bezpečnostních mechanismů. Bezpečnostní funkce poskytované v rámci UN/EDIFACT standardu zaručují bezpečnost způsobem end-to-end, to znamená od jednoho koncového uživatele k druhému, nezávisle na způsobu přenosu zpráv (zprávy mohou být přenášeny v nezabezpečených veřejných komunikačních sítích). Uplatněné bezpečnostní mechanismy se stávají součástí struktury UN/EDIFACT zpráv, a pokud jsou tyto zprávy archivovány, může být kdykoli po dobu archivace ověřena integrita a autentičnost zprávy. Základní prvky UN/EDIFACT bezpečnostního standardu, které jsou využity pro zabezpečení EDI zpráv v systému jsou následující:

V rámci standardu UN/EDIFACT jsou definovány standardní struktury, které umožňují využití digitálního podpisu přímo v UN/EDIFACT zprávách. Každá zpráva, která je opatřena digitálním podpisem, obsahuje tzv. úvodní bezpečnostní segmenty (Security Header), které obsahují údaje o algoritmech použitých pro digitální podpis, způsob vytvoření digitálního podpisu a certifikát uživatele, a dále tzv. závěrečné bezpečnostní segmenty (Security Trailer), které obsahují výsledek autentizace zprávy - tedy samotný digitální podpis. Postup při tvorbě digitálního podpisu je následující: nejprve je ke zprávě vytvořen kontrolní blok bytů pomocí tzv. hash funkce. Tento kontrolní blok má tu vlastnost, že je unikátní pro každou zprávu. Kontrolní blok je potom zašifrován tajným klíčem odesilatele zprávy a zašifrovaný blok je připojen ke zprávě.

Standard UN/EDIFACT definuje zprávu CIPHER, která umožňuje přenos šifrovaných údajů. UN/EDIFACT zpráva je zašifrovaná od počátečního segmentu až ke koncovému segmentu a vložena do těla zprávy CIPHER, tak je zaručena důvěrnost přenášených dat.

UN/EDIFACT standard definuje zprávu AUTACK. Tato zpráva odpovídá na došlou zprávu a obsahuje referenci a vypočtený kontrolní blok bytů, které jsou unikátní pro každou došlou zprávu. Zpráva je opatřena digitálním podpisem příjemce, takže ten nemůže později popřít doručení zprávy.

V rámci UN/EDIFACT standardu je definována zpráva KEYMAN, která umožňuje přenášet klíče a certifikáty mezi různými aplikacemi.

Certifikační autorita - význam a funkce

Pro fungování systému digitálního podpisu je třeba, aby každému oprávněnému uživateli EDI byly známy veřejné klíče ostatních oprávněných uživatelů, s kterými komunikuje. O šíření veřejných klíčů mezi uživateli a jejich správu se stará Certifikační autorita (CA). Naopak je nutné, aby tajný klíč byl znám pouze svému vlastníkovi.

Certifikační autorita přiděluje účastníkům certifikáty, což jsou v podstatě potvrzení o veřejném klíči uživatele. Certifikáty jsou v elektronické podobě a jsou podepsány pomocí tajného klíče CA. Veřejný klíč CA je všeobecně znám, takže každý si může ověřit platnost libovolného certifikátu. Certifikát obsahuje: číslo certifikátu, identifikaci vlastníka, dobu zahájení platnosti, dobu ukončení platnosti a veřejný klíč vlastníka. Certifikát (nebo pouze jeho referenční číslo) je posílán s podepsanou zprávou a pomocí veřejného klíče, který je v něm obsažen je ověřována platnost použitého digitálního podpisu. Bez platného certifikátu nelze tedy digitální podpis používat.

Standard UN/EDIFACT definuje přesný tvar certifikátu. Díky tomu je možné propojení různých systémů založených na tomto standardu s tím, že vzájemně mohou být uznávány certifikáty uživatelů a digitální podpisy zpráv.

Certifikační autorita, kromě přidělování certifikátů, udržuje seznam platných certifikátů, archivuje certifikáty, kterým prošla doba platnosti, a udržuje tzv. Black List (nebo též Certificate Revocation List) , kde jsou certifikáty formálně platné, ale fakticky je jejich platnost zrušena. CA také rozšiřuje seznamy platných certifikátů a Black List mezi uživatele.

Kromě těchto základních funkcí může CA plnit i další funkce, které úzce souvisí s bezpečností systému. CA může plnit funkce tzv. Důvěryhodné třetí strany (Trusted Third Party), která díky svému technickému a "společenskému" kreditu může vykonávat různé důležité funkce v EDI systémech jako je např. tzv. elektronický notář (Electronic Notary), potvrzování funkčnosti, navazování spojení a uznávání certifikátů s jinými certifikačními autoritami (cross-certification), vydávání potvrzení o autentičnosti dat (witnessing), aj.

Řešení na straně obchodních partnerů

Díky tomu, že systém zabezpečení přenosu EDI zpráv je založen na mezinárodních normách, otevírá se uživatelům tohoto systému široká škála možných implementací - od jednoduchých PC aplikací až k náročným aplikacím, které umožňují implementaci bezpečnostních mechanismů přímo v existujícím systému uživatele. Kromě daného rozhraní systému nelze předepsat způsob implementace. V dalších odstavcích je naznačeno několik možných způsobů řešení, které rozhodně nepokrývají celou šíři možností. Je nutné si uvědomit, že při rozsáhlejších aplikacích bude nejvhodnější individuální přístup.

Řešení - základní popis

Řešení je založeno na následujících základních principech:

a) Formální a strukturální řešení implementace bezpečnostních funkcí je založeno na doporučení UN/TRADE/WP.4/R.1026 a ISO/CD 9735-5,6. Toto řešení zajišťuje korektní a přitom otevřenou implementaci bezpečnostních funkcí integrity zprávy, sekvenční integrity zpráv, autentizace a neodmítnutí.

b) Jako základní metodu pro implementaci požadovaných základních bezpečnostních funkcí je použit tzv. digitální podpis, který zajistí kromě silně vyžadovaných funkcí integrity a autentizace i funkce neodmítnutí. Pro tento systém jsou využity následující algoritmy:

* asymetrický algoritmus RSA s modulem klíče 1024
* hash funkce MD5, ev. další hash algoritmy

Tyto algoritmy jsou běžně dostupné a jsou již implementovány v řadě bankovních aplikací. Jejich implementace a používání je podchyceno i mezinárodními normami.

c) Jako další bezpečnostní funkce definované v doporučeních pro UN/EDIFACT je použita zpráva CIPHER (zajištění důvěrnosti zpráv) a zpráva AUTACK (zajištění neodmítnutí příjmu zprávy). Zpráva CIPHER využívá hybridní metody šifrování, kdy text zprávy je šifrován algoritmem DES (mód CBC) s náhodně zvoleným klíčem , který je šifrován algoritmem RSA a odeslán spolu se zprávou. Zpráva AUTACK je generována příjemcem a informuje původního odesílatele o bezchybném příjmu zprávy, eventuálně o chybě vzniklé při příjmu.

d) Správa klíčů bude založena na certifikaci veřejných klíčů. Je to v podstatě jediná metoda, která umožňuje plné využití všech výhod digitálního podpisu, poskytuje efektivní metodu správy klíčů i pro větší systémy (více než 50 uživatelů) a dává všem účastníkům stejné záruky bezpečnosti. Certifikace klíčů bude Certifikační Autoritou, tato by měla zajišťovat centrální správu klíčů pro různé EDI aplikace.

V rámci správy klíčů se provádí tyto základní funkce:

* dvojice klíčů si generuje každý uživatel sám
* uživatel má k dispozici certifikát lokální(ch) aplikace(í)
* aplikace CA provádí certifikace veřejných klíčů
* aplikace CA provádí registrace certifikátů
* aplikace CA ruší certifikáty
* aplikace CA udržuje databáze platných a zrušených certifikátů

Technická implementace

V této kapitole je podrobně popsána implementace výše uvedených bezpečnostních funkcí.

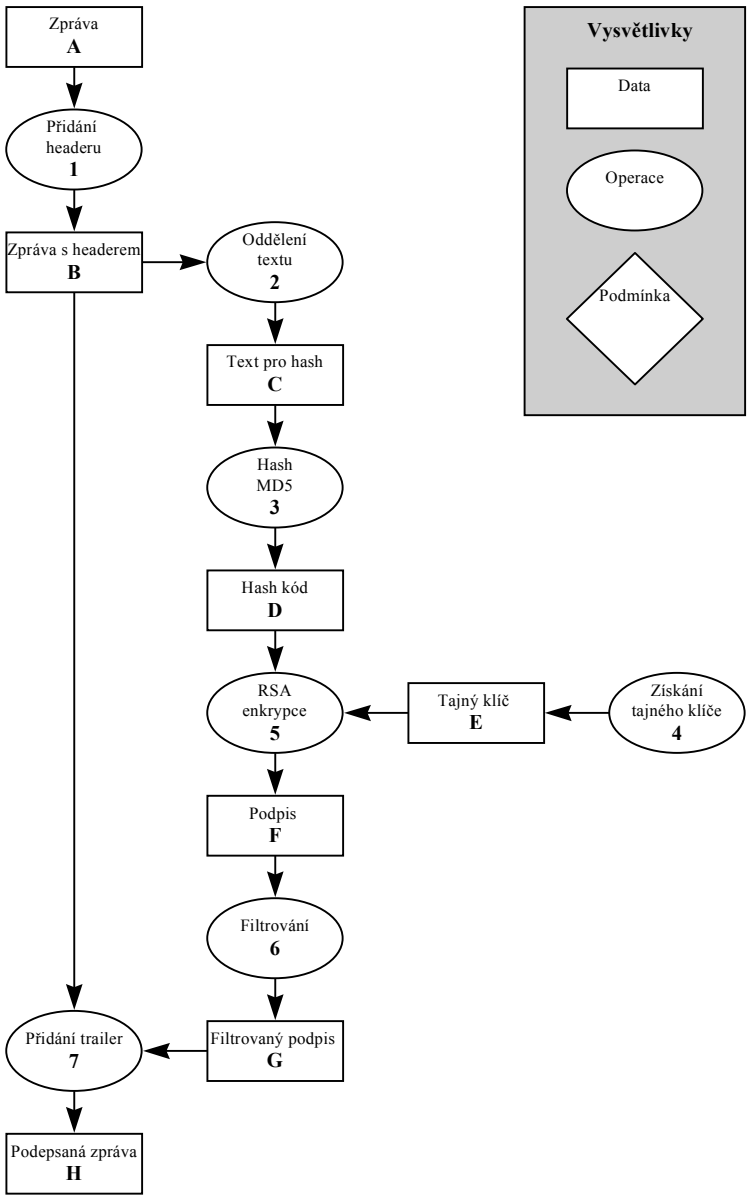
Implementace digitálního podpisu

Princip tvorby a kontroly digitálního podpisu

Digitální podpis zprávy slouží pro zabezpečení jedné zprávy. V případě, že soubor výměny obsahuje více zpráv, zabezpečuje se každá zpráva zvlášť.

Na následujícím schématu je uveden princip tvorby digitálního podpisu pro jednu zprávu:

OBR. 2 - Schéma tvorby podpisu



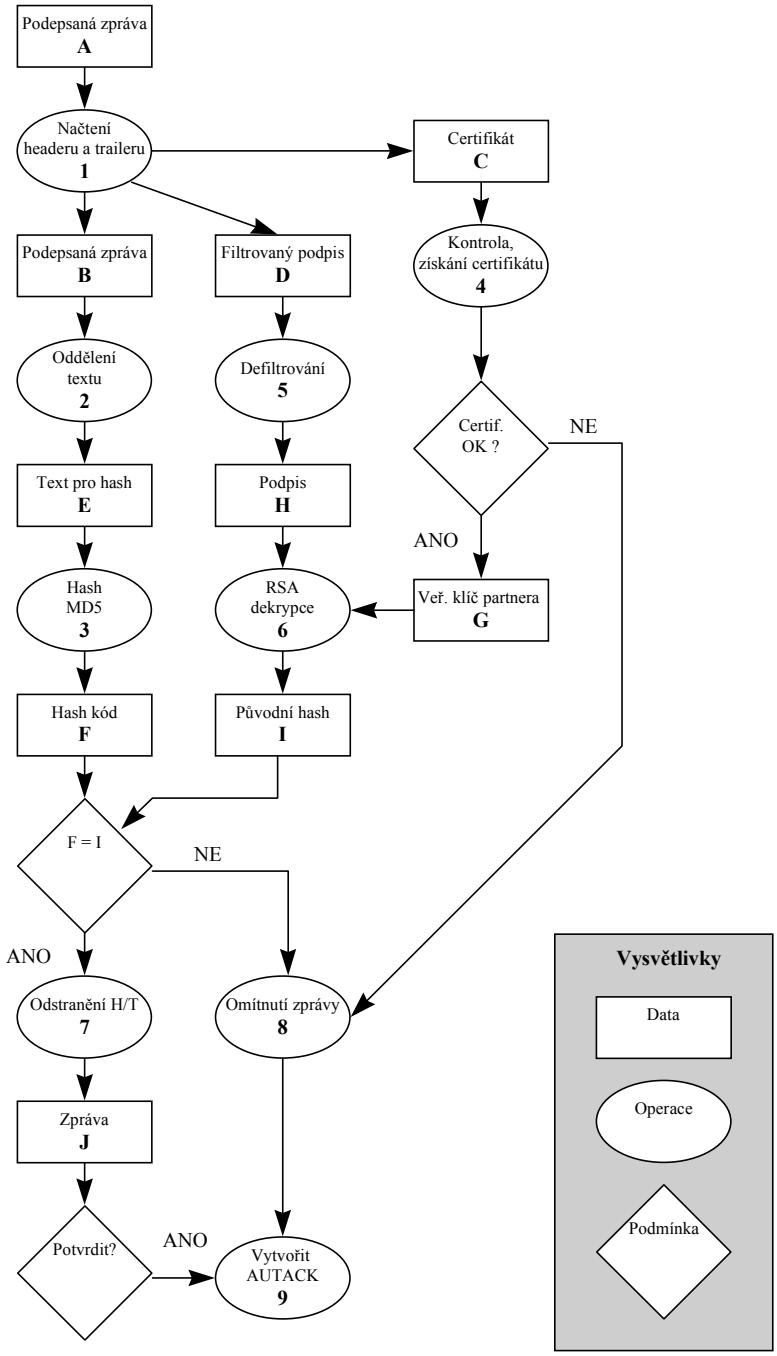
Postup při tvorbě podpisu je následující:

1. Do UN/EDIFACT zprávy [A] jsou přidány vyplněné úvodní bezpečnostní segmenty (bezpečnostní header).
2. Ze zprávy s bezpečnostním headerem [B] je získán text, který bude vstupem do hash funkce (tedy úvodní bezpečnostní segmenty nejprve, a potom samotné tělo zprávy). Výsledkem je souvislý text [C], který je reprezentován jako posloupnost bytů.
3. Text [C] je zpracován MD5 hash funkcí, výsledkem je 16 bytový hash kód [D].
4. Je získán tajný klíč uživatele [E] potřebný pro vytvoření podpisu.

5. Hash kód [D] je zašifrován RSA algoritmem pomocí tajného klíče [E]. Výsledkem je digitální podpis [F] o délce odpovídající modulu klíče v takovém tvaru, že první byte (index 0) odpovídá nejvyššímu řádu čísla.
6. Digitální podpis [F] je filtrován to textové podoby, tak aby mohl být přenášen v UN/EDIFACT zprávě.
7. Do zprávy jsou přidány koncové bezpečnostní segmenty (bezpečnostní trailer), které obsahují filtrovaný podpis [G]. Výsledkem je kompletní zabezpečená zpráva [H].

Na následujícím schématu je uveden princip kontroly digitálního podpisu pro jednu zprávu:

OBR. 3 - Schéma kontroly podpisu



Postup při kontrole podpisu je následující:

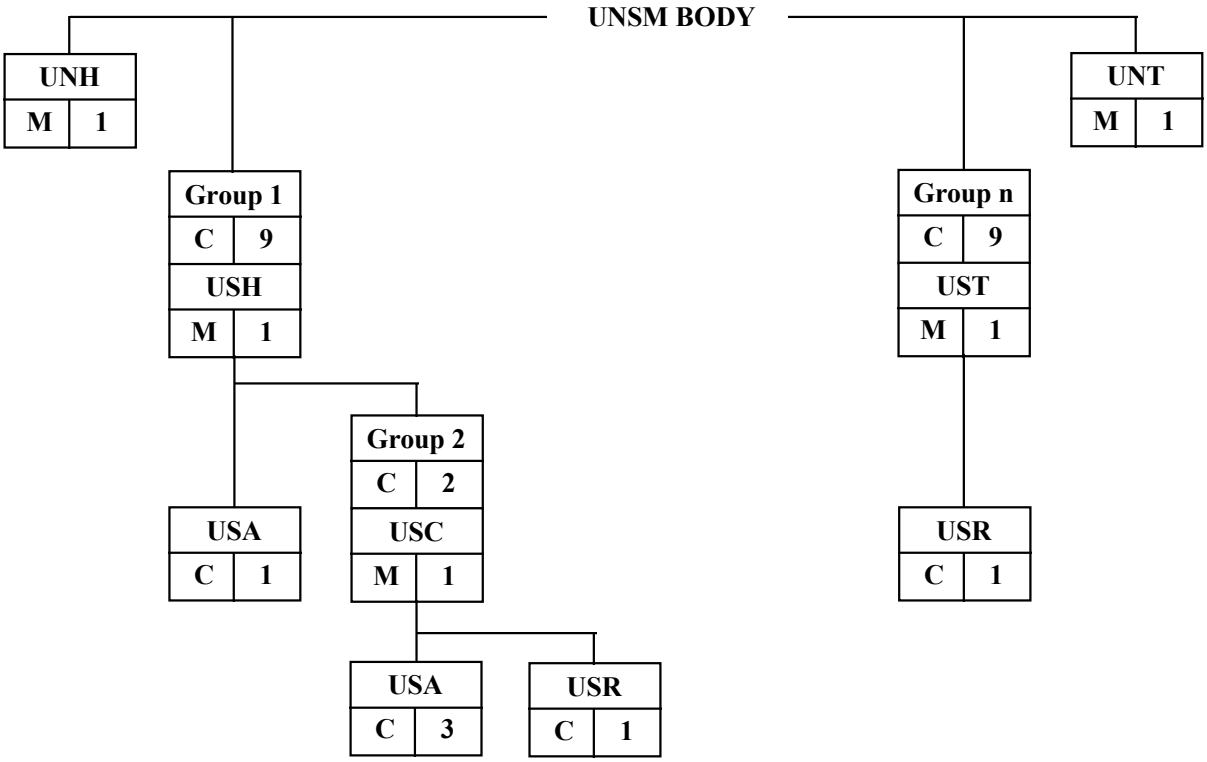
1. Z podepsané zprávy [A] jsou načteny údaje uvedené v úvodních (header) a koncových (trailer) bezpečnostních segmentech.

2. Z podepsané zprávy [B] je získán text, který bude vstupem do hash funkce (tedy úvodní bezpečnostní segmenty nejprve, a potom samotné tělo zprávy). Výsledkem je souvislý text [E], který je reprezentován jako posloupnost bytů.
3. Text [E] je zpracován MD5 hash funkcí, výsledkem je 16 bytový hash kód [F].
4. Z headeru byl načteno číslo certifikátu [C], certifikát pak musí být načten z lokální databáze, certifikát může být podle potřeby ověřen a z certifikátu je získán veřejný klíč partnera [G] potřebný pro ověření zprávy. V headeru mohl být uveden i kompletní certifikát [C], v tomto případě je certifikát ověřen a z něj je získán veřejný klíč partnera [G].
5. Z traileru byl načten filtrovaný digitální podpis [D], tento musí být zpětně defiltrován do binární podoby.
6. Digitální podpis [H] je dešifrován algoritmem RSA pomocí veřejného klíče partnera [G]. Výsledkem je původní hash kód zprávy [I] o délce 16 bytů.
7. Pokud byla úspěšná kontrola podpisu (tj. vypočtený hash kód se rovná původnímu), jsou ze zprávy odstraněny úvodní a koncové segmenty, vznikne tedy "čistá" zpráva [J].
8. Pokud nebyla úspěšná kontrola podpisu (tj. vypočtený hash kód se rovná původnímu) nebo nebyl úspěšně zkontrolován certifikát (chybný podpis certifikátu, certifikát neplatný, certifikát není k dispozici aj.), musí být zpráva odmítnuta a nesmí být dále zpracována.
9. Pokud zpráva má být potvrzena nebo je odmítnuta, je vytvořena potvrzovací zpráva AUTACK pro odesílatele původní zprávy (podrobnosti viz kapitola Implementace zprávy AUTACK).

Syntaktická pravidla a formální pravidla pro digitální podpis

Mechanismus zabezpečení UN/EDIFACT zpráv pomocí digitálního podpisu je navržen na základě doporučení UN/TRADE/WP.4/R.1026/Add.2 a ISO/CD 9735-5. Formálně je digitální podpis implementován pomocí úvodních a koncových služebních bezpečnostních segmentů. Pro každou UN/EDIFACT zprávu jsou přidány pro zabezpečení speciální segmenty, struktura zabezpečené zprávy je na obr. 2. Tyto segmenty umožňují vytvoření až 9 digitálních podpisů pro jednu zprávu. V implementaci se počítá s jedním podpisem. Pokud je při příjmu zprávy zjištěna chyba v digitálním podpisu, je generována zpráva AUTACK (viz další odstavec), která je odeslána původci přijímané zprávy, musí být zároveň informován příjemce/aplikace příjemce a událost zapsána do příjemcova log souboru.

OBR. 4 - Struktura zabezpečené UN/EDIFACT zprávy



Segmenty UNH a UNT jsou standardní služební segmenty zabezpečované zprávy (Message Header, Message Trailer). UNSM Body je tělo zabezpečované zprávy, počínaje segmentem BGM a dále všechny ostatní segmenty.

Určité bezpečnostní segmenty (USR,USA) obsahují data, která jsou výsledkem kryptografických funkcí nebo slouží jako vstup do těchto funkcí. Tyto data mohou být obecně binární (tj. každý byte dat může být v rozsahu 0 - 255). Proto, aby mohla být tato data uvedena v EDIFACT segmentu, musí být nejprve zpracována pomocí tzv. filtrovací funkce (někdy se též tyto funkce nazývají kódovací), která převede binární data do jiné reprezentace, kdy data jsou již reprezentována pomocí zobrazitelných znaků a tím pádem mohou být uvedena v EDIFACTu. Naopak pokud jsou tato data z EDIFACTu čtena, musí být opět zpracována filtrovací funkcí, která zpětně ze znakové reprezentace vytvoří data v původní binární podobě. Nejjednodušším příkladem filtru je hexadecimální filtr, který každý byte binárních dat reprezentuje pomocí dvojice znaků ('0' - 'F'), tedy např. číslo 125163 je reprezentováno jako posloupnost znaků '1', 'E', '8', 'E', 'B'.

Rozsah zabezpečení zprávy (tj. vstup do hash funkce) je následující: Security Header (všechny segmenty skupiny 1 a 2), od prvního znaku segmentu USH tj. 'U' do znaku oddělovače posledního segmentu Security Header (tj. ' ' ') včetně a tělo zprávy (následuje za

Security Header) do znaku oddělovače posledního segmentu těla včetně (segment bezprostředně před UST).

Význam a popis bezpečnostních segmentů je v tab. 1

TAB. 1 Popis bezpečnostních segmentů

M/C - **povinný (M)** - jedná se o prvek nebo segment, skupinu, které jsou definovány jako povinné standardem a tím pádem jsou povinné i pro implementaci bezpečnostních segmentů

- **použitý nepovinný (C)** - jedná se o prvek nebo segment, skupinu, které jsou sice definovány ve standardu jako nepovinné, ale v implementaci jsou použity, jejich použití je tedy povinné

- **běžně nepoužívaný (O)** - jedná se o prvek nebo segment, skupinu, které jsou definovány ve standardu jako nepovinné a v implementaci nejsou zatím používány, zde jsou buď vynechány, nebo jsou definovány pro budoucí použití nebo pro kompatibilitu s dalšími standardními systémy. Jejich eventuální využití neovlivní základní bezpečnostní funkce systému a jednotlivé implementace je mohou využívat pro své specifické účely.

Op. - počet opakování, v závorce je uveden maximální počet povolený standardem. V () je uvedeno opakování, které nebude využito, v [] jsou uvedeny opakování, které lze využít v jiných implementacích.

SKUPINA SEGMENT	M/C	Op.	POPIS
1	C	1[9]	Tato skupina segmentů slouží k identifikaci použitých bezpečnostních služeb.
USH	M	1	Definuje speciální bezpečnostní služby použité pro danou zprávu, obsahuje časovou značku a údaje o stranách poskytujících bezpečnostní služby.
USA	C	1	Algoritmus použitý pro hashing zprávy
2	C	1(2)	Skupina segmentů 2 představuje certifikát odesílající strany
USC	M	1	Obsahuje číslo certifikátu, identifikaci vlastníka certifikátu, dobu platnosti certifikátu, datum vydání certifikátu a další údaje
USA	C	1[3]	Obsahuje údaje o algoritmu, který vlastník používá pro digitální podpis, a veřejný klíč vlastníka.
USR	C	1	Podpis certifikátu vytvořený tajným klíčem CA
N	C	1[9]	V této skupině je výsledek autentizace celé zprávy
UST	M	1	Segment slouží k označení části zprávy, na kterou je uplatněn daný bezpečnostní mechanismus, a k propojení výsledku autentizace s daným USH segmentem.
USR	C	1	Digitální podpis zprávy pomocí tajného klíče

Pozn. Číslování skupin je nezávislé od číslování skupin v těle zprávy.

Podrobný popis jednotlivých segmentů a jejich struktury je v tab. 2

TAB. 2 Struktura bezpečnostních segmentů

S.Prv. - Číslo složeného prvku v UN/EDIFACT Standard Directory
Prvek - Číslo prvku v UN/EDIFACT Standard Directory
P. - povinný (M), použitý nepovinný (C), běžně nepoužívaný (O) segment, prvek
Formát - specifikace formátu dle konvencí UN/EDIFACT
Obsah - v ' ' jsou uváděny konstanty, textové identifikátory odkazují na proměnné hodnoty dodávané bezpečnostní aplikací

Pozn.: Pokud se vyskytují opakované segmenty nebo opakované složené prvky, není jejich význam (a tím i obsah) určen pořadím výskytu, ale patřičnými kvalifikátory obsaženými v složeném prvku nebo segmentu.

SKUPINA 1 (C,1 - 9) SEGMENT USH (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0552	M	an..3	Verze struktury segmentů	'94W'	Verze z roku 1994
	0501	M	an..3	Bezp. funkce - kód	'1'	Neodmítnutí původu
	0534	M	an..14	Kontrolní reference	link	link=01 pro jeden podpis
	0541	C	an..3	Rozsah zabezpečení - kód	'1'	úvodní bezp. segmenty + tělo zprávy
	0503	C	an..3	Typ odpovědi, kód	ack	ack= '1' - zpráva nemá být potvrzena zprávou AUTACK ack= '2' - zpráva má být potvrzena zprávou AUTACK
	0505	C	an..3	Filtr (funkce) - kód	filter	Filtr pro binární data
	0507	C	an..3	Kódování znaků -kód	'2'	ASCII 8 bitů
	0509	C	an..3	Role podep. strany - kód	'1'	Původce dokumentu
S500		*O*		*Identifikace strany*		*Identifikace odesílající strany*
S500	0577	M	an..3	Kvalifikátor strany	'1'	Odesílatel zprávy
S500	0538	C	an..35	Jméno klíče	key	key = číslo (jméno) klíče použitého pro podpis
S500	0511	C	an..17	ID strany	EDI_ID	EDI_ID= identifikace EDI aplikace odesílatele
S500	0513	O	an..3	Použitý seznam stran	'1'	Kód seznamu partnerů (EDI aplikací)
S500	0515	O	an..3	Agentura udržující seznam	'CNB'	Kód agenturry udržující seznam
S500	0586	O	an..35	Jméno strany	org_name	org_name= jméno organizace
S500	0586	O	an..35	Jméno strany	org_dep	org_dep= oddělení (pobočka) v organizaci
S500	0586	O	an..35	Jméno strany	org_pers	org_pers= odpovědný pracovník
S500		*O*		*Identifikace strany*		*Vynecháno*
	0520	C	an..35	Referenční číslo	ref_num	ref_num= sekvěční referenční číslo

S501		*C*		*Datum a čas*		*Časová značka - vytvoření podpisu*
S501	0517	M	an..3	Kvalifikátor datumu a času	'1'	Bezpečnostní časová značka
S501	0338	C	n..8	Datum	date	date= datum vytvoření podpisu, formát YYYYMMDD
S501	0314	C	n..15	Čas	time	time= čas vytvoření podpisu, formát HHMMSS
S501	0336	O	n4	UTC offset (odchylka času)	offset	offset = '0100' - odchylka od UTC je + 1 hod (zimní čas) offset = '0200' - odchylka od UTC je + 2 hod (letní čas)

Skupina segmentů 1 definuje parametry pro digitální podpis zprávy a spolu se skupinou n také tvoří digitální podpis zprávy. Skupina 1 se spolu se skupinou n opakuje pro každý digitální podpis zprávy. Pro současnou aplikaci se počítá pouze s jedním podpisem, tedy i s jedním opakováním skupin.

Popis prvků:

0552 - Verze struktury segmentů
Hodnota '94W' definuje, že jsou použity služební bezpečnostní segmenty popsané v dokumentu UN/TRADE/WP.4/R.1026 a ISO/CD 9735-5.

0501 - Bezpečnostní funkce
Pro zabezpečení zpráv je použito funkce neodmítnutí původu (hodnota '1')

0534 - Kontrolní reference
Tento prvek slouží jako jednoznačný klíč pro spojení skupin 1 (Security Header) a n (Security Trailer) - tzn. parametry definované ve skupině 1 se vztahují na skupinu n, která má stejnou hodnotu prvku 0534. Hodnota prvku je dvoumístná numerická. Pro tuto aplikaci se počítá s jedním digitálním podpisem - hodnota link je tedy '01'. Pro další opakování skupin (více podpisů) se link inkrementuje.

0541 - Rozsah zabezpečení
Hodnota '1' definuje, že podpis je vypočítán z textu úvodních bezpečnostních segmentů (skupina 1 a 2) - od prvního písmene segmentu USH (tj. 'U') do oddělovače ukončujícího tyto segmenty včetně a z textu těla zprávy, který je bezprostředně připojen - od prvního znaku za oddělovačem ukončujícím úvodní bezpečnostní segmenty (tedy 'B' ze segmentu BGM) až do separátoru před koncovými bezpečnostními segmenty včetně. V případě jednoho podpisu to znamená, že se aplikuje hash funkce na souvislý text od 'U' segmentu USH až k ' ' ' před segmentem UST. V případě více podpisů se aplikuje hash funkce pouze na jednu aktuální skupinu úvodních bezpečnostních segmentů (tj. skupiny 1 a 2) a tělo zprávy, to znamená, že podpisy jsou nezávislé a nejsou hierarchicky řazeny .

0503 - Typ odpovědi
Tento prvek určuje, zda odesílatel požaduje od příjemce funkci neodmítnutí příjmu - tj. potvrzení zprávy pomocí AUTACK; ack může mít dvě hodnoty:
'1' - odesílatel nepožaduje potvrzení zprávou AUTACK
'2' - odesílatel požaduje potvrzení.

0505 - Filtr (funkce)
Určuje typ funkce, která je použita pro filtrování binárních dat, která jsou výsledkem digitálního podpisu, před jejich zápisem do zprávy (do prvku S508:0560 v segmentu USR skupina n).
Pro filtrování je možné využít buď hexadecimální filtr, nebo filtr definovaný v ISO 9735-5 (též v R.1026) tzv. UNO-A filtr, oba plně vyhovují UN/EDIFACT syntaktické úrovni A (jsou tedy universální). Vybraný filtr se potom používá na všechna binární data ve zprávě (kromě certifikátu, kde je definován filtr pro certifikát).
Hexadecimální filtr reprezentuje jeden byte dvojicí znaků ('0' - '9', 'A' -'F'), první znak reprezentuje vrchní 4 bity, druhý spodní. V hexadecimálním zápisu představují levé znaky významnější byty. Nevýznamné nuly zleva mohou být vynechány.
Kód filter má následující hodnoty:
'2' - hexadecimální filtr
'5' - UNO-A filtr

0507 - Kódování znaků
Určuje kódování znaků EDIFACT zprávy před aplikací digitálního podpisu. Zde je použito 8 bitové ASCII (hodnota '2'), znamená to, že zpráva musí být v tomto kódování, když se vytváří nebo kontroluje digitální podpis.

0509 - Role podepisující strany
viz tabulka

S500 - Identifikace strany (první opakování)
Slouží pro jednoznačnou identifikaci strany, která vytvořila digitální podpis zprávy. Obsahuje údaje o identitě strany a identifikaci klíče použitého pro podpis. Vzhledem k tomu, že identické údaje jsou uvedeny v certifikátu, nemusí být uveden.

S500:0577 - Kvalifikátor strany
viz tabulka

S500:0538 - Jméno klíče
Obsahuje identifikaci uživatelova tajného klíče použitého pro digitální podpis. Hodnota key musí být jednoznačná pro všechny uživatelovy klíče, jak platné, tak i zrušené (doporučeno je inkrementální číslování klíčů). Hodnota key musí být shodná s hodnotou prvku v certifikátu veřejného klíče (S500:0538 v segmentu USC) pro danou dvojici klíčů, tak aby bylo možné párovat použitý tajný klíč s odpovídajícím certifikátem veřejného klíče.

S500:0511 - ID strany
Obsahuje identifikaci organizace pro EDI. Hodnotu EDI_ID přiděluje EDIVAN. EDI_ID identifikuje organizaci (stranu) v EDI komunikaci a může být odlišný (v případě, že organizace užívá více EDI aplikací) od identifikace aplikace v segmentu UNB (prvky S002:0004 a S003:0010). Tato identifikace slouží především pro účely správy klíčů, díky ní je možné, aby se např. v organizaci používal jeden klíč pro více EDI aplikací . Mapování mezi EDI_ID (které je pouze jedno pro organizaci) a identifikací aplikace z UNB (kdy organizace může mít libovolný počet aplikací, různě identifikovaných) musí být provedeno v implementaci.

S500:0513 - Použitý seznam stran
S500:0515 - Agentura udržující seznam
Pro současnou aplikaci se počítá pouze s jedním seznamem, není tedy třeba hodnoty uvádět, hodnoty uvedené v tabulce jsou pokládány za defaultní. Jejich využití se předpokládá později, pokud bude lokálně používáno více EDI aplikací.

S500:0586 Jméno strany
Určeno pro detailnější specifikaci strany. V současné aplikaci nebudou podrobněji využity. Předpokládá se především využití pokud uživatel bude vlastnit více klíčů nebo provozovat více EDI aplikací.

S500 - Identifikace strany (druhé opakování)
Tento prvek je vynechán.

0520 - Referenční číslo
Tento prvek obsahuje referenční číslo, které slouží pro kontrolu sekvence podepsaných zpráv. Hodnota ref_num je numerická, je unikátní pro daného uživatele pro všechny odeslané zprávy a je inkrementována pro každou odeslanou zprávu. Je doporučeno (pokud je to možné) používat zde referenční číslo zprávy (segment UNH prvek 0062).

S501 - Datum a čas
Tento prvek definuje datum a čas vytvoření podpisu zprávy. Tento prvek spolu s prvkem 0520 slouží pro zajištění integrity sekvence zpráv.
Pozn.: Hodnoty prvků S501 se řídí normou ISO 8601, u UTC offsetu (0336) se neuvádí '+' pro kladné hodnoty (je to UN/EDIFACT separátor).

S501:0517 - Kvalifikátor datumu a času
viz tabulka

S501:0338 - Datum
Hodnota date musí mít předepsaný formát YYYYMMDD (např. 19950403).

S501:0314 - Čas
Hodnota time musí mít předepsaný formát HHMMSS (např. 182033). Hodnota time představuje běžný čas používaný v České republice.

S501:0336 - UTC offset
Tento prvek slouží pro rozlišení letního a zimního času. Hodnota offset udává odchylku lokálního času od standardního světového času, to znamená pro zimní čas + 1 hodina (hodnota '0100') a pro letní čas + 2 hodiny (hodnota '0200').

Pozn. Nesprávné časové údaje mohou ovlivnit některé bezpečnostní funkce, proto je nezbytné, aby čas byl správně uváděn v souladu s platným časem.

SKUPINA 1 (C, 1 - 9)SEGMENT USA (C, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S502		*M*		*Bezp. algoritmus*		*Algoritmus pro hash zprávy*
S502	0523	M	an..3	Použití algoritmu - kód	'1'	Algoritmus je použit pro hashing zprávy
S502	0525	C	an..3	Operační mód - kód	'0'	Pro daný algoritmus nemá význam
S502	0533	O	an..3	Seznam operačních módů	'1'	Seznam definovaný UN/EDIFACT SJWG
S502	0527	C	an..3	Algoritmus - kód	'6'	Algoritmus MD5 (Rivest, Dusse - RSA Security Inc., 1991)
S502	0529	O	an..3	Seznam algoritmů	'1'	Seznam definovaný UN/EDIFACT SJWG
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*

Popis prvků:

S502 - Bezpečnostní algoritmus
Prvek popisuje uživatelův algoritmus použitý na hashing zprávy pro vytvoření digitálního podpisu.

S502:0523 - Použití algoritmu
viz tabulka
S502:0525 - Operační mód
viz tabulka

S502:0533 - Seznam operačních módů
Prvek definuje použitý seznam operačních módů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S502:0527 - Algoritmus
Prvek definuje použitý algoritmus. Podrobná specifikace algoritmu a jeho parametrů je v kapitole Parametry použitých kryptografických algoritmů.

S502:0529 - Seznam algoritmů
Prvek definuje použitý seznam algoritmů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S503 - Parametry algoritmu
Tyto prvky nejsou využity, algoritmus MD5 nepotřebuje žádné vstupní parametry.

SKUPINA 2 (C, 1) SEGMENT USC (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0536	C	an..35	Ref. číslo certifikátu	ref_num	ref_num= referenční číslo certifikátu - unikátní
S500		*C*		*Identifikace strany*		*Identifikace vlastníka certifikátu*
S500	0577	M	an..3	Kvalifikátor strany	'3'	Vlastník certifikátu
S500	0538	C	an..35	Jméno klíče	key1	key1= číslo (jméno) certifikovaného klíče
S500	0511	C	an..17	ID strany	EDI_ID	EDI_ID= EDI identifikace organizace vlastníka klíče
S500	0513	O	an..3	Použitý seznam stran	'1'	Kód seznamu partnerů (EDI aplikací)
S500	0515	O	an..3	Agentura udržující seznam	'CNB'	Kód agenturry udržující seznam
S500	0586	O	an..35	Jméno strany	org_name1	org_name1= jméno organizace
S500	0586	O	an..35	Jméno strany	org_dep1	org_dep1= oddělení (pobočka) v organizaci
S500	0586	O	an..35	Jméno strany	org_pers1	org_pers1= odpovědný pracovník
S500		*C*		*Identifikace strany*		*Identifikace Certifikační autority*
S500	0577	M	an..3	Kvalifikátor strany	'4'	CA, strana potvrzující platnost certifikátu
S500	0538	C	an..35	Jméno klíče	key2	key2= číslo (jméno) klíče pro podpis certifikátu
S500	0511	C	an..17	ID strany	CA_ID	CA_ID= identifikace CA
S500	0513	O	an..3	Použitý seznam stran	'1'	Kód seznamu CA
S500	0515	O	an..3	Agentura udržující seznam	'CNB'	Kód agenturry udržující seznam
S500	0586	O	an..35	Jméno strany	org_name2	org_name2= jméno organizace CA
S500	0586	O	an..35	Jméno strany	org_dep2	org_dep2= oddělení (pobočka) v organizaci
S500	0586	O	an..35	Jméno strany	org_pers2	org_pers2= odpovědný pracovník
	0544	C	an..3	Verze formátu certifikátu	'94W'	Verze z roku 1994
	0505	C	an..3	Filtr (funkce) - kód	filter	filter = '2' Filtr pro binární data

	0507	C	an..3	Kódování znaků - kód	'2'	ASCII 8 bitů
	0543	C	an..3	Výběr znaků - kód	'4'	UN/EDIFACT úroveň syntaxe D
	0546	O	an..35	Úroveň práv	rights	rights= stavové slovo, definuje práva vlastníka
S505		*O*		*Oddělovače*		*Oddělovače použité při podpisu certifikátu*
S505 S505	0550 0551	C C	an..4 an..3	Separátor Kvalifikátor separátoru	'27' '1'	Oddělovač ' ' ' Oddělovač segmentů
S505		*O*		*Oddělovače*		*Oddělovače použité při podpisu certifikátu*
S505 S505	0550 0551	C C	an..4 an..3	Separátor Kvalifikátor separátoru	'2B' '2'	Oddělovač ' + ' Oddělovač datových prvků
S505		*O*		*Oddělovače*		*Oddělovače použité při podpisu certifikátu*
S505 S505	0550 0551	C C	an..4 an..3	Separátor Kvalifikátor separátoru	'3A' '3'	Oddělovač ' : ' Oddělovač ve složených datových prvcích
S505		*O*		*Oddělovače*		*Oddělovače použité při podpisu certifikátu*
S505 S505	0550 0551	C C	an..4 an..3	Separátor Kvalifikátor separátoru	'3F' '1'	Oddělovač ' ? ' Uvolňovací znak
S501		*C*		*Datum a čas*		*Datum a čas pro certifikát*
S501 S501 S501 S501	0517 0338 0314 0336	M C C O	an..3 n..8 n..15 n..4	Kvalifikátor datumu a času Datum Čas UTC offset (odchylka času)	'2' nebo '6' date1 time1 offset1	Vytvoření/zrušení certifikátu date1= datum, formát YYYYMMDD time1= čas, formát HHMMSS offset1 = '0100' - odchylka od UTC je + 1 hod (zimní čas) offset1 = '0200' - odchylka od UTC je + 2 hod (letní čas)
S501		*C*		*Datum a čas*		*Datum a čas pro certifikát*
S501 S501 S501 S501	0517 0338 0314 0336	M C C O	an..3 n..8 n..15 n4	Kvalifikátor datumu a času Datum Čas UTC offset (odchylka času)	'3' date2 time2 offset2	Začátek platnosti od date2= datum, formát YYYYMMDD time2= čas, formát HHMMSS offset 2= '0100' - odchylka od UTC je + 1 hod (zimní čas) offset 2= '0200' - odchylka od UTC je + 2 hod (letní čas)

S501		*C*		*Datum a čas*		*Datum a čas pro certifikát*
S501	0517	M	an..3	Kvalifikátor datumu a času	'4'	Platí do
S501	0338	C	n..8	Datum	date3	date3= datum, formát YYYYMMDD
S501	0314	C	n..15	Čas	time3	time3= čas, formát HHMMSS
S501	0336	O	n4	UTC offset (odchylka času)	offset3	offset3 = '0100' - odchylka od UTC je + 1 hod (zimní čas) offset3 = '0200' - odchylka od UTC je + 2 hod (letní čas)
	0567	C	an..3	Bezpečnostní status	status	status= status certifikátu

Skupina segmentů 2 představuje certifikát uživatele. Ve zprávě se opakuje skupina 2 pouze jednou. Tento certifikát je vytvořen kompletně Certifikační autoritou při certifikaci veřejného klíče. V certifikátu jsou uvedeny jednak údaje dodané uživatelem jako je identifikace uživatele, identifikace klíče, veřejný klíč uživatele aj. a dále údaje dodané při certifikaci jako je referenční číslo certifikátu, časové údaje o platnosti aj. Certifikát nelze následně měnit, údaje v něm slouží pouze pro získání údajů souvisejících s digitálním podpisem.
Certifikát je opatřen digitálním podpisem Certifikační autority. Způsob digitálního podpisu certifikátu je podobný digitálnímu podpisu zprávy. Nejprve je text certifikátu zpracován hash funkcí (MD5), jejíž výsledkem je krátký kontrolní blok bytů. Rozsah textu certifikátu, který je vstupem do hash funkce je následující: od prvního znaku segmentu USC (tedy 'U') k oddělovači segmentů (znak ' ' ') za posledním opakováním segmentu USA (míněno ve skupině 2) včetně. Následně je kontrolní blok bytů šifrován algoritmem RSA pomocí tajného klíče CA a tento výsledek je potom uvedený filtrovaný v segmentu USR skupiny 2.
Certifikát může být poslán se zprávou kompletní (tj. celá skupina 2), nebo je posláno pouze referenční číslo certifikátu (v případě, že druhá strana již má patřičný certifikát), tedy pouze segment USC s jediným prvkem 0536. Certifikáty mezi jednotlivými stranami se vyměňují způsobem popsaným v kapitole Správa klíčů.

Popis prvků

0536 - Referenční číslo certifikátu
Tento prvek obsahuje referenční číslo certifikátu. Hodnota ref_num je unikátní pro všechny certifikáty v systému, jak platné, tak neplatné. Prvek je vyplněn při certifikaci.

S500 - Identifikace strany (první opakování)
Slouží pro jednoznačnou identifikaci vlastníka certifikátu. Obsahuje údaje o identitě vlastníka, které dodá uživatel spolu s veřejným klíčem pro certifikaci klíče, dále obsahuje identifikaci veřejného klíče.

S500:0577 - Kvalifikátor strany
viz tabulka

S500:0538 - Jméno klíče
Obsahuje identifikaci uživatelova veřejného klíče obsaženého v certifikátu. Hodnota key1 musí být jednoznačná pro všechny uživatelovy klíče, jak platné, tak i zrušené (doporučeno je inkrementální číslování klíčů).

S500:0511 - ID strany
Obsahuje identifikaci organizace pro EDI. Hodnotu EDI_ID přiděluje EDIVAN. EDI_ID identifikuje organizaci (stranu) v EDI komunikaci a může být odlišný (v případě, že organizace užívá více EDI aplikací) od identifikace aplikace v segmentu UNB (prvky S002:0004 a S003:0010). Tato identifikace slouží především pro účely správy klíčů, díky ní je možné, aby se např. v organizaci používal jeden klíč pro více EDI aplikací . Mapování mezi EDI_ID (které je pouze jedno pro organizaci) a identifikací aplikace z UNB (kdy organizace může mít libovolný počet aplikací, různě identifikovaných) musí být provedeno v implementaci.

S500:0513 - Použitý seznam stran
S500:0515 - Agentura udržující seznam
Pro současnou aplikaci se počítá pouze s jedním seznamem, hodnoty tedy nebudou uvedeny; hodnoty uvedené v tabulce jsou pokládány za defaultní. Jejich využití se předpokládá později, pokud bude více lokálních EDI aplikací.

S500:0586 Jméno strany
Určeno pro detailnější specifikaci strany. Hodnoty jsou v prvcích uvedeny pouze tehdy, pokud je uživatel dodá k certifikaci. Předpokládá se především využití pokud uživatel bude vlastnit více klíčů, nebo provozovat více EDI aplikací.

S500 - Identifikace strany (druhé opakování)
Tento prvek je určen pro identifikaci Certifikační autority, tj. strany, která provedla digitální podpis certifikátu. Celý tento prvek je vyplněn při certifikaci.

S500:0577 - Kvalifikátor strany
viz tabulka

S500:0538 - Jméno klíče
Obsahuje identifikaci veřejného klíče CA z páru, který byl použit pro digitální podpis certifikátu. key2 spolu s CA_ID slouží pro identifikaci certifikátu klíče CA, který má být použit pro kontrolu podpisu certifikátu.

S500:0511 - ID strany
Obsahuje identifikaci CA. Tato identifikace slouží pro účely správy klíčů, formálně je shodná s EDI_ID organizace.

S500:0513 - Použitý seznam stran
S500:0515 - Agentura udržující seznam
Pro současnou aplikaci se počítá pouze s jedním seznamem, hodnoty tedy nebudou uvedeny; hodnoty uvedené v tabulce jsou pokládány za defaultní. Jejich využití se předpokládá později, pokud bude více lokálních EDI aplikací.

S500:0586 Jméno strany
Určeno pro detailnější specifikaci CA. Zatím nebudou tyto prvky využity.

0544 - Verze formátu certifikátu
Hodnota '94W' definuje, že pro certifikát jsou použity služební bezpečnostní segmenty popsané v dokumentu UN/TRADE/WP.4/R.1026 a ISO/CD 9735 - 5. Prvek je vyplněn při certifikaci.

0505 - Filtr (funkce)
Určuje typ funkce, která je použita pro filtrování binárních dat, která jsou výsledkem digitálního podpisu certifikátu (prvek S508:0560, segment USR, skupina 2), a binárních dat reprezentujících uvedený klíč (prvek S503:0532, segment USA, skupina 2), před jejich zápisem do certifikátu .
Pro filtrování se používá hexadecimální filtr (kód = '2'), filtr se potom používá na všechna binární data v certifikátu.
Hexadecimální filtr reprezentuje jeden byte dvojicí znaků ('0' - '9', 'A' -'F'), první znak reprezentuje vrchní 4 bity, druhý spodní. V hexadecimálním zápisu představují levé znaky významnější byty. Nevýznamné nuly zleva mohou být vynechány.

0507 - Kódování znaků
Určuje kódování znaků použitých pro zápis segmentů certifikátu před aplikací digitálního podpisu. Zde je použito 8 bitové ASCII (hodnota '2'), znamená to, že certifikát je v tomto kódování, když Certifikační autorita vytváří jeho podpis. Prvek je vyplněn při certifikaci.

0543 - Výběr znaků
Tento prvek určuje výběr sady znaků pro segmenty certifikátu. Zde je určeno, že jsou použity znaky podle UN/EDIFACT syntaktické úrovně D (hodnota '4'). Vzhledem k tomu, že pro aplikaci SÚD se používá standardně syntaktická úroveň D, nebude zatím tento prvek využit, hodnota '4' bude pokládána za defaultní. Jeho využití se předpokládá později, pokud bude více lokálních EDI aplikací, nebo pro specifické případy.

0546 - Úroveň práv
Tento prvek definuje stavové slovo, které určuje využití klíče obsaženého v certifikátu, práva vlastníka klíče aj. Hodnota rights je alfanumerická, předepsaného formátu, první znak zleva je povinný, ostatní jsou nepovinné; formát rights je:
'AB-CCCC-DDDD..' kde
'A' - je znak, který určuje využití klíče, má následující hodnoty:
'A' - klíč je určen pro digitální podpis a šifrování symetrických klíčů
'B' - klíč je určen pouze pro digitální podpis

'C' - klíč je určen pouze pro šifrování symetrických klíčů
'Z' - klíč má jiné využití

'B' - je znak , který definuje úroveň práv uživatele, má hodnoty v rozsahu '0' - '9' kdy:
'0' - nejnižší úroveň práv
'1' - '8' - odstupňované vyšší úrovně práv
'9' - nejvyšší úroveň práv

'-' - je oddělovací znak, vyskytuje se pouze pokud za ním vpravo následují další znaky

'C' - jsou čtyři znaky vyhrazené pro budoucí potřebu

'-' - je oddělovací znak, vyskytuje se pouze pokud za ním vpravo následují další znaky

'D' - jsou znaky dodané vlastníkem certifikátu, slouží pro jeho potřebu, zde může být až 27 znaků.

Tento prvek není v dosavadní aplikaci použit, předpokládá se jeho defaultní hodnota 'A0', která odpovídá využití klíčů pro aplikaci SÚD. Později se předpokládá jeho využití pro uživatele, kteří budou vlastnit více klíčů, nebo pokud bude více lokálních EDI aplikací.

S505 - Oddělovače
Tyto prvky nejsou využity, používají se standardní oddělovače (které taky představují default). Později se počítá s jejich využitím pro specifické aplikace.

S501 - Datum a čas (první opakování)
Tento prvek obsahuje datum a čas vytvoření certifikátu (kvalifikátor 0517 = '2') nebo datum a čas zrušení certifikátu (kvalifikátor 0517 = '6'). Údaje doplňuje certifikační autorita při vytvoření/zrušení certifikátu.

S501:0517 - Kvalifikátor datumu a času
viz tabulka

S501:0338 - Datum
Hodnota date1 musí mít předepsaný formát YYYYMMDD (např. 19950403).

S501:0314 - Čas
Hodnota time1 musí mít předepsaný formát HHMMSS (např. 182033). Hodnota time představuje běžný čas používaný v České republice.

S501:0336 - UTC offset
Tento prvek slouží pro rozlišení letního a zimního času. Hodnota offset1 udává odchylku lokálního času od standardního světového času, to znamená pro zimní čas + 1 hodina (hodnota '0100') a pro letní čas + 2 hodiny (hodnota '0200').

S501 - Datum a čas (druhé opakování)
Tento prvek obsahuje datum a čas začátku platnosti certifikátu. Údaje doplňuje certifikační autorita při vytvoření certifikátu. Popis jednoduchých prvků viz výše.

S501 - Datum a čas (třetí opakování)
Tento prvek obsahuje datum a čas ukončení platnosti certifikátu. Údaje doplňuje certifikační autorita při vytvoření certifikátu. Popis jednoduchých prvků viz výše.

0567 - Bezpečnostní status
Tento prvek určuje status certifikátu, pokud je certifikát platný není tento prvek uveden a platí jeho defaultní hodnota '1' (viz níže). Hodnota status může být následující:
'1' - certifikát je platný
'2' - certifikát je zrušen (bezpečnostní důvody)
'3' - status certifikátu je neznámý
'4' - certifikát je ukončen (ukončen z formálních důvodů)
'5' - certifikát je podezřelý
'6' - certifikát vypršel

SKUPINA 2 (C, 1) SEGMENT USA (C, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S502		*M*		*Bezp. algoritmus*		*Algoritmus pro digitální podpis vlastníka certifikátu*
S502	0523	M	an..3	Použití algoritmu - kód	'6' nebo '7'	Algoritmus je použit pouze digitální podpis zprávy (kód '6') nebo pro podpis zprávy a šifrování symetrického klíče (kód '7')
S502	0525	C	an..3	Operační mód - kód	'0'	Pro daný algoritmus nemá význam
S502	0533	O	an..3	Seznam operačních módů	'1'	Seznam definovaný UN/EDIFACT SJWG
S502	0527	C	an..3	Algoritmus - kód	'10'	Algoritmus RSA(Rivest, Shamir, Adleman,1978)
S502	0529	O	an..3	Seznam algoritmů	'1'	Seznam definovaný UN/EDIFACT SJWG
S503		*C*		*Parametry algoritmu*		*Parametry pro RSA*
S503	0532	C	an..512	Hodnota parametru	length	length= délka modulu,
S503	0531	C	an..3	Kvalifikátor param. - kód	'14'	dekadicky
S503		*C*		*Parametry algoritmu*		*Parametry pro RSA*
S503	0532	C	an..512	Hodnota parametru	exp	exp= exponent pro algoritmus RSA, filtrováno
S503	0531	C	an..3	Kvalifikátor param. - kód	'13'	exponent veřejného klíče
S503		*C*		*Parametry algoritmu*		*Parametry pro RSA*
S503	0532	C	an..512	Hodnota parametru	mod	mod= modulus pro algoritmus RSA, filtrováno
S503	0531	C	an..3	Kvalifikátor param. - kód	'12'	modulus veřejného klíče
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*

Tento segment obsahuje veřejný klíč vlastníka certifikátu a parametry algoritmu, pro který je klíč určen.

Popis prvků:

S502 - Bezpečnostní algoritmus
Prvek popisuje uživatelův asymetrický šifrovací algoritmus (RSA) používaný pro digitální podpis zpráv odesílaných uživatelem (kód 0523 = '6') nebo používaný pro digitální podpis a zároveň pro šifrování symetrických klíčů (kód 0523 = '7').

S502:0523 - Použití algoritmu
viz tabulka

S502:0525 - Operační mód
viz tabulka

S502:0533 - Seznam operačních módů
Prvek definuje použitý seznam operačních módů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S502:0527 - Algoritmus
Prvek definuje použitý algoritmus. Podrobná specifikace algoritmu a jeho parametrů je definována v kapitole Parametry použitých kryptografických algoritmů.

S502:0529 - Seznam algoritmů
Prvek definuje použitý seznam algoritmů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S503 - Parametry algoritmu (první výskyt)
Tento prvek definuje délku modulu pro RSA algoritmus. Délka modulu je definována v kapitole Parametry použitých kryptografických algoritmů.

S503:0532 - Hodnota parametru
Hodnota length udává délku modulu v bitech. Hodnota je uvedena dekadicky, tj. hodnota je '1024'.

S503:0531 - Kvalifikátor parametru
viz tabulka

S503 - Parametry algoritmu (druhý výskyt)
Tento prvek definuje exponent veřejného klíče vlastníka certifikátu pro RSA algoritmus.

S503:0532 - Hodnota parametru
Hodnota exp představuje exponent veřejného klíče. Hodnota je uvedena filtrovaná (viz popis prvku 0505 v segmentu USC). Pro používaný fixní exponent (Fermatovo číslo F4) je tedy hodnota exp '10001' hexadecimálně.

S503:0531 - Kvalifikátor parametru
viz tabulka

S503 - Parametry algoritmu (třetí výskyt)
Tento prvek definuje exponent veřejného klíče vlastníka certifikátu pro RSA algoritmus.

S503:0532 - Hodnota parametru
Hodnota mod představuje modulus veřejného klíče. Hodnota je uvedena filtrovaná (viz popis prvku 0505 v segmentu USC).

S503:0531 - Kvalifikátor parametru
viz tabulka

S503 - Parametry algoritmu (další výskyty)
Tyto prvky nejsou využity, pro algoritmus RSA není třeba dalších parametrů.

SKUPINA 2 (C, 1) SEGMENT USA (O, 2)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S502		*M*		*Bezp. algoritmus*		*Algoritmus pro hash certifikátu (provádí CA)*
S502	0523	M	an..3	Použití algoritmu - kód	'4'	Algoritmus je pro hashing certifikátu
S502	0525	C	an..3	Operační mód - kód	'0'	Pro daný algoritmus nemá význam
S502	0533	O	an..3	Seznam operačních módů	'1'	Seznam definovaný UN/EDIFACT SJWG
S502	0527	C	an..3	Algoritmus - kód	'6'	Algoritmus MD5 (Rivest, Dusse - RSA Security Inc., 1991)
S502	0529	O	an..3	Seznam algoritmů	'1'	Seznam definovaný UN/EDIFACT SJWG
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*

Tento segment obsahuje popis algoritmu použitého Certifikační autoritou na hash certifikátu pro jeho digitální podpis. Tento segment je v aplikaci SÚD nevyužit, neboť se předpokládá standardní využití algoritmu MD5. Hodnoty uvedené v tabulce představují defaultní hodnoty prvků pro tento účel.

SKUPINA 2 (C, 1) SEGMENT USA (O, 3)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S502		*M*		*Bezp. algoritmus*		*Algoritmus pro podpis certifikátu (provádí CA)*
S502	0523	M	an..3	Použití algoritmu - kód	'3'	Algoritmus je digitální podpis certifikátu
S502	0525	C	an..3	Operační mód - kód	'0'	Pro daný algoritmus nemá význam
S502	0533	O	an..3	Seznam operačních módů	'1'	Seznam definovaný UN/EDIFACT SJWG
S502	0527	C	an..3	Algoritmus - kód	'10'	Algoritmus RSA(Rivest, Shamir, Adleman,1978)
S502	0529	O	an..3	Seznam algoritmů	'1'	Seznam definovaný UN/EDIFACT SJWG
S503		*C*		*Parametry algoritmu*		*Parametry pro RSA*
S503	0532	C	an..512	Hodnota parametru	length	length= délka modulu,
S503	0531	C	an..3	Kvalifikátor param. - kód	'14'	dekadicky
S503		*C*		*Parametry algoritmu*		*Parametry pro RSA*
S503	0532	C	an..512	Hodnota parametru	exp	exp= exponent pro algoritmus RSA, filtrováno
S503	0531	C	an..3	Kvalifikátor param. - kód	'13'	exponent veřejného klíče
S503		*C*		*Parametry algoritmu*		*Parametry pro RSA*
S503	0532	C	an..512	Hodnota parametru	mod	mod= modulus pro algoritmus RSA, filtrováno
S503	0531	C	an..3	Kvalifikátor param. - kód	'12'	modulus veřejného klíče
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*

Tento segment obsahuje popis asymetrického šifrovacího (RSA) algoritmu použitého Certifikační autoritou pro vytvoření digitálního podpisu certifikátu a také veřejný klíč CA, který používá pro podpis certifikátu. Tento segment je využit výjimečně v certifikátu veřejného klíče CA, kdy segment nahrazuje USA segment s veřejným klíčem subjektu (prakticky to však znamená pouze změnu kvalifikátoru S502:0523 v USA segmentu obsaženém v certifikátu). Certifikát veřejného klíče CA je šířen metodou popsanou v kapitole Správa klíčů.

SKUPINA 2 (C, 1) SEGMENT USR (C, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S508		*M*		*Výsledek bezp. funkce*		*Digitální podpis certifikátu*
S508	0560	M	an..256	Výsledná hodnota	sig_val	sig_val = výsledek dig. podpisu, filtrováno
S508	0560	O	an..256	Výsledná hodnota		Vynecháno

Popis prvků:

S508 - Výsledek bezpečnostní funkce
Obsahuje výsledek digitálního podpisu certifikátu.

S508:0560 - Výsledná hodnota (první výskyt)
Hodnota sig_val obsahuje výsledek digitálního podpisu ve filtrované(textové) podobě (viz popis prvku 0505 v segmentu USC).

S508:0560 - Výsledná hodnota (druhý výskyt)
Prvek není použit.

SKUPINA n (C, 1 - 9) SEGMENT UST (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0534	M	an..14	Kontrolní reference	link	link='01' pro jeden podpis

Popis prvků:

0534 - Kontrolní reference
Tento prvek slouží jako jednoznačný klíč pro spojení skupin 1 (Security Header) a n (Security Trailer) - tzn. parametry definované ve skupině 1 se vztahují na skupinu n, která má stejnou hodnotu prvku 0534. Pro tuto aplikaci se počítá s jedním digitálním podpisem - hodnota link je tedy '01'. Pro další opakování skupin (více podpisů) se link inkrementuje.

SKUPINA n (C, 1 - 9) SEGMENT USR (C, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S508		*M*		*Výsledek bezp. funkce*		*Digitální podpis zprávy*
S508	0560	M	an..256	Výsledná hodnota	sig_val	sig_val = výsledek dig. podpisu, filtrováno
S508	0560	O	an..256	Výsledná hodnota		Vynecháno

Výsledek podpisu obsažený v tomto segmentu je svázán s parametry v segmentu USH a s certifikátem (skupina 2) pomocí segmentu UST (viz výše).

Popis prvků:

S508 - Výsledek bezpečnostní funkce
Obsahuje výsledek digitálního podpisu zprávy.

S508:0560 - Výsledná hodnota (první výskyt)
Hodnota sig_val obsahuje výsledek digitálního podpisu v filtrované(textové) podobě (viz popis prvku 0505 v segmentu USH).

S508:0560 - Výsledná hodnota (druhý výskyt)
Prvek není použit.

Příklad podepsané zprávy

Příklad souboru výměny s podepsanou zprávou (přestože jsou zde segmenty odděleny pro přehlednost CRLF, v reálném souboru výměny následují přímo za sebou):

Segmenty	Komentář
UNB+UNOD:2+BANK+CNBASUD+960521:2002+000010033'	Hlavička souboru výměny, jedná se o soubor výměny od aplikace BANK pro aplikaci CNBASUD.
UNH+236+GESMES:D:95A:UN'	Hlavička zprávy, jedná se o zprávu GESMES, její referenční číslo je 236.
USH+94W+1+01+1+2+2+2+1+++236+1:19960521:200246:0200' USA+1:0:1:6:1' USC+CATEST000000021'	Úvodní bezpečnostní segmenty. USH segment definuje především typ funkce (digitální podpis), referenci podpisu (01), požadavek na potvrzení (kód 2), použitou filtr funkci (hexadecimální), bezpečnou kopii ref. čísla zprávy, timestamp vytvoření podpisu. Segment USA definuje použitou hash funkci (MD5). Segment USC obsahuje odkaz na certifikát, který musí být použit při kontrole podpisu.
BGM+:::Vydání výskytu výkazu+ZKUS_96.01+X05' DTM+137:960521:102' DSI+ROSIFE20.04.00.197' STS+X09+X01' ARR+X00+6700' ARR+X00+19960331' ARR+X00+1' ARR+X00+30000000.00' ARR++2' ARR++40000000.00' ARR++3' ARR++30000000.00'	Vlastní tělo zprávy, tvoří jej uživatelské segmenty, které byly ve zprávě i před zabezpečením.
UST+01' USR+64E13B655B71EEEA17353D99A443B9BF015A6C2BF856A3B38DAB0502D0F00AB7C44EA791A39F4295A17B3D2130FD8E273BD93444C03847C7C8A7CE8DB17EA8D6786D94209C6654CE947BDC7FDA3B0ED331E2520B8C76AA262E60F8B66FC5A85520F368A617875750805E00E6482FFFE7615C73561C815B271AAAF07E3E24F0B1'	Koncové bezpečnostní segmenty. Segment UST svazuje koncové bezpečnostní segmenty s úvodními pomocí reference podpisu (01). Segment USR obsahuje samotný digitální podpis zprávy ve filtrované podobě.
UNT+19+236'	Patička zprávy, zpráva obsahuje 19 segmentů (včetně služebních).
UNZ+1+000010033'	Patička souboru výměny, soubor výměny obsahuje 1 zprávu.

Příklad certifikátu, který je referován ve zprávě (tj. musí být použit pro kontrolu zprávy):

Segmenty	Komentář
USC+CATEST000000021+3:BANK_KEY1:BANK::: ::OWNER+4:CA_KEY0:CA+94W+2+2+4++++++2:1 9951215:093243:0200+3:19960101:000000:0100+4:1 9960701:000000:02000'	USC segment obsahuje číslo certifikátu (CATEST000000021), identifikaci organizace (BANK) a vlastníka certifikátu (OWNER), klíče vlastníka (BANK_KEY1), identifikaci CA (CA), klíče CA použitého pro podpis certifikátu (CA_KEY0), typ filtru pro veřejný klíč a podpis a dále datumy a časy vytvoření certifikátu , začátku platnosti certifikátu a konce platnosti certifikátu.
USA+7:0:1:10:1+1024:14+010001:13+C1164701726 B49F75B9CAB59E0BF9F28657D78ADCA738EC70 EF256F9657272602ABD32E4F4AF731F0BC4515D9 EE1B07638E1CBDB94D791A7463DE2E2AC62B009 040B9F4E7D47B5EF9594E91E4D3136421D876BC5 552C4A87BD4DB14C6A271C257C71A6D44F3E342 7D03CE9D36B0904D50834C5B99E31A7815E11CE1 7ED8AD2CD:12'	Segment USA definuje uživatelův algoritmus pro podpis (RSA) a obsahuje jeho veřejný klíč, hodnoty jsou filtrovány : délka klíče 1024 bitů , exponent (010001H) a modulus (C1164...H) klíče.
USR+61098948944B7A62BA67389DEB73273D4DD A56BCCE593F4E2CA32870E09ECB3833ADCDA27 6B92D329C6E051BBDEF6B90529EAEF16D096356 292EB6CC14EFFCA912006EE6536BB5593E8C6BC 8EC156A64A88C518394A1DE60109FEDA9C4A36B 6EA37D9F1CDD5A21698A4176C767E3D5F5C6CF9 ED765DF5AFBC81DFCC098F3F6F7'	Segment USR obsahuje podpis certifikátu, který je uveden filtrovaný.

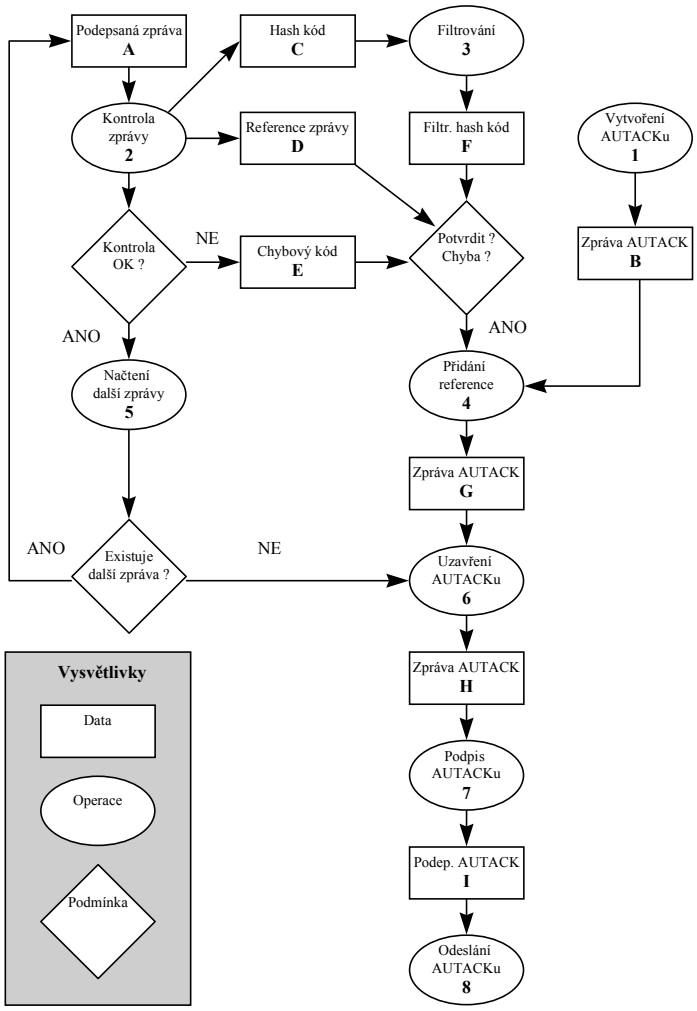
Implementace zprávy AUTACK

Princip použití zprávy AUTACK

Zpráva AUTACK je potvrzovací zpráva a slouží pro bezpečné potvrzení příjmu určité zprávy nebo pro informování o bezpečnostní chybě při kontrole zprávy. Zpráva AUTACK obsahuje reference na přijaté zprávy a hash kód přijatých zpráv (tzv. otisk zprávy, fingerprint), hash kód slouží pro neodmítnutí obsahu zprávy. Zpráva AUTACK je opatřena podpisem příjemce původní zprávy, podpis zabezpečení funkci neodmítnutí příjmu zprávy. AUTACK může potvrzovat i více zpráv.

Na následujícím obrázku je ukázáno vytvoření potvrzovací zprávy AUTACK pro zprávy přijaté v rámci jednoho souboru výměny:

OBR. 5 - Schéma vytvoření zprávy AUTACK



Postup při vytvoření AUTACKu je následující:

1. Pokud mají být nějaké přijaté zprávy potvrzeny, je vytvořen soubor výměny, který je určen pro odesílatele zpracovávaného souboru výměny. Tento obsahuje zprávu AUTACK [B], do které budou vloženy potřebné reference (viz dále).
2. Z přijatého souboru výměny je získána a zkontrolována jedna podepsaná zpráva [A]. Výsledkem kontroly (viz kapitola Implementace digitálního podpisu) je hash kód zprávy [C], reference zprávy [D], pokud je při kontrole zprávy zjištěna chyba, je určen kód chyby [E].
3. Hash kód [C] je filtrován do textové podoby tak, aby mohl být přenášen v UN/EDIFACT zprávě.
4. Pokud kontrolovaná zpráva má být potvrzena (určeno v úvodních bezpečnostních segmentech) nebo byla zjištěna při kontrole zprávy chyby, je přidána reference dané zprávy [D] spolu s filtrovaným hash kódem [C] (pokud byl vygenerován) a kódem chyby [E] (pokud se jedná o chybu) do těla zprávy AUTACK [B].
5. Po zkontrolování zprávy je načtena další podepsaná zpráva ze souboru výměny, zpráva je opět zkontrolována a potvrzena podle bodů 2 - 4. Pokud v souboru výměny již není další podepsaná zpráva, postupuje se dále podle bodu 6.
6. Zpráva AUTACK [G] je uzavřena.
7. Zpráva AUTACK [H] je opatřena digitálním podpisem příjemce pomocí standardního postupu (viz kapitola Implementace digitálního podpisu).
8. Podepsaná zpráva AUTACK [I] je odeslána původci zkontrolovaného souboru výměny.

Odesílatel původní zprávy si může ověřit z referencí a otisku původní zprávy, že zpráva byla přijata korektně, kontrolou podpisu AUTACKu (dle kapitoly Implementace digitálního podpisu) ověří, že zpráva byla přijata určenou stranou. AUTACK mu slouží jako důkaz o příjmu nebo z kódu chyby zjistí příčinu, proč zpráva nebyla dále zpracována.

Syntaktická pravidla a formální pravidla pro zprávu AUTACK

Zpráva AUTACK je implementována podle doporučení UN/EDIFACT UN/TRADE/WP.4/R.1026/Add.3 a Add.4 a podle ISO/CD 9735-6.

Tato zpráva informuje odesílatele libovolné zprávy o výsledku ověření bezpečnostních funkcí zprávy příjemcem. Zpráva AUTACK odpovídá na došlou zprávu, která měla nastaven požadavek na potvrzení (prvek 0503 v segmentu USH - tzn. že přijatá zpráva musí být podepsána, viz kapitola Implementace digitálního podpisu), a poskytuje tak funkci neodmítnutí příjmu, informuje tedy odesílatele, že jeho zpráva byla přijata a že byl ověřen její podpis, AUTACK již neřeší věcnou správnost přijaté zprávy, k tomu je určen speciální protokol na aplikační úrovni. AUTACK může také sloužit jako hlášení o chybě při kontrole zabezpečení zprávy nebo při dešifrování zprávy, v tomto případě musí být patřičně vyplněn kód chyby v prvku S508:571 segmentu USY ve skupině 3 vztahující se k referované zprávě.

Zpráva AUTACK, pokud slouží pro potvrzení příjmu, musí obsahovat hash kód přijaté zprávy (prvek S560:571 segmentu USY ve skupině 3 vztahující se k referované zprávě), tento je vytvořen při kontrole podpisu zprávy postupem popsaným v kapitole Implementace digitálního podpisu. Pokud zpráva AUTACK informuje o chybě zabezpečení, obsahuje hash kód pouze tehdy, mohl-li být vytvořen. Hash kód uvedený ve zprávě AUTACK je filtrovaný stejným algoritmem, jaký byl použit pro filtrování podpisu přijaté zprávy.

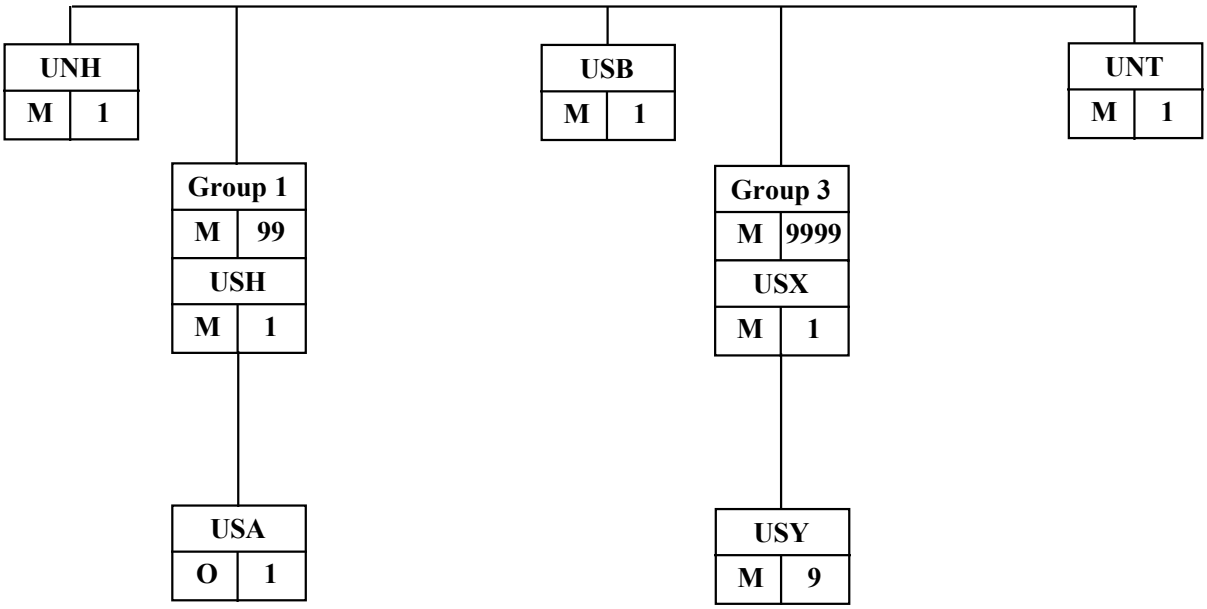
Zpráva AUTACK a soubor výměny obsahující zprávu AUTACK jsou vytvořeny mimo pořadí běžné výměny zpráv. Je nutné zajistit, aby referenční číslo tohoto souboru výměny nekolidovalo s referenčními čísly běžných souborů výměny. Referenční číslo souboru výměny (prvek 0020 v segmentu UNB) má proto doporučený specifický tvar, kdy se skládá z tzv. prefixu a vlastního čísla. Prefix je pevný řetězec znaků 'AUTACK', vlastní číslo je dekadická znaková reprezentace celého čísla (může obsahovat nuly vlevo pro zarovnání délky), přiřazeného danému souboru výměny, kdy se toto číslo inkrementuje pro každý nový soubor výměny s AUTACK zprávou, prvotní hodnota je 1. Příklad takového referenčního čísla je 'AUTACK0023'.

Zpráva AUTACK musí být vždy opatřena digitálním podpisem příjemce původní zprávy (tj. původce AUTACKu). Zpráva AUTACK se zabezpečuje pomocí úvodních a koncových bezpečnostních segmentů jako kterákoli jiná zpráva (viz kapitola Implementace digitálního podpisu), znamená to že pro podpis jsou do zprávy přidány ještě úvodní a koncové bezpečnostní segmenty.

Zpráva AUTACK může odpovídat na více došlých zpráv, zprávy ale musí být součástí jednoho souboru výměny.

Zpráva AUTACK se již opět nepotvrzuje zprávou AUTACK (možnost cyklu).

OBR. 6 - Struktura zprávy AUTACK



Význam a popis segmentů je v tab. 3

TAB. 3 Popis bezpečnostních segmentů
M/C - povinný (M), použitý nepovinný (C), běžně nepoužívaný (O) segment (skupina)
Op. - počet opakování, v závorce je uveden maximální počet povolený standardem. V () je uvedeno opakování, které nebude využito, v [] jsou uvedeny opakování, které lze využít v jiných implementacích.

Podrobný popis jednotlivých segmentů, jejich struktury je v tab. 4

SKUPINA SEGMENT	M/C	Op.	POPIS
1	M	1(99)	Tato skupina segmentů slouží k identifikaci použitého bezpečnostního mechanismu pro odpověď na přijatou zprávu
USH	M	1	Definuje bezpečnostní služby použité pro odpověď na přijatou zprávu
USA	O	1	Algoritmus použitý pro hashing přijaté zprávy
USB	M	1	Poskytuje identifikaci zúčastněných stran a obsahuje časovou značku.
3	M	1(9999)	Definuje zprávy, na které AUTACK odpovídá a výsledek bezpečnostních funkcí uplatněných při příjmu
USX	M	1	Obsahuje odkazy na přijatou zprávu
USY	M	1(9)	Obsahuje výsledky zpracování zprávy

TAB. 4 Struktura segmentů zprávy AUTACK

S.Prv. - Číslo složeného prvku v UN/EDIFACT Standard Directory
Prvek - Číslo prvku v UN/EDIFACT Standard Directory
P. - povinný (M), použitý nepovinný (C), běžně nepoužívaný (O) segment, prvek
Formát - specifikace formátu dle konvencí UN/EDIFACT
Obsah - v ' ' jsou uváděny konstanty, textové identifikátory odkazují na proměnné hodnoty dodávané bezpečnostní aplikací

SEGMENT UNH (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0062	M	an..14	Ref. číslo zprávy	ref_no	ref_no = ref. číslo, jednoznačné
S009		*M*		*Identifikátor zprávy*		*Identifikuje typ UN/EDIFACT zprávy*
S009	0065	M	an..6	Typ zprávy	'AUTACK'	
S009	0052	M	an..3	Verze zprávy	'D'	
S009	0054	M	an..3	Číslo verze	'94A'	
S009	0051	M	an..2	Odpovědná agentura	'UN'	
S009	0057	O	an..6	Speciální kód		Vynecháno
	0068	O	an..35	Společná reference		Vynecháno
S010		*O*		*Stav přenosu*		*Vynecháno*

Segment UNH je standardní služební segment, který využívají všechny UN/EDIFACT zprávy, jeho použití se řídí standardními pravidly UN/EDIFACT.

SKUPINA 1 (M,1) SEGMENT USH (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0552	M	an..3	Verze struktury segmentů	'94W'	Verze z roku 1994
	0501	M	an..3	Bezp. funkce - kód	'5'	Neodmítnutí příjmu
	0534	M	an..14	Kontrolní reference	'00'	Číslo 00 (aby nebyla kolize s USH přijmuté zprávy)
	0541	O	an..3	Rozsah zabezpečení - kód	'1'	Úvodní bezp. segmenty + tělo zprávy 1)
	0503	O	an..3	Typ odpovědi - kód		Vynecháno
	0505	O	an..3	Filtr (funkce) - kód	filter	Filtr pro binární data 1)
	0507	O	an..3	Kódování znaků -kód	'2'	ASCII 8 bitů 1)
	0509	O	an..3	Role strany - kód	'1'	Původce dokumentu
S500		*O*		*Identifikace strany*		*Vynecháno*
S500		*O*		*Identifikace strany*		*Vynecháno*
	0516	O	an..35	Referenční číslo		Vynecháno
S501		*O*		*Datum a čas*		*Vynecháno*

1) Tyto prvky kopírují prvky ze Security Header přijaté zprávy, není tedy třeba je uvádět, původci zprávy jsou implicitně známy.

Skupina 1 obsahuje údaje o funkci zprávy AUTACK a parametry pro vytvoření potvrzovacích referencí. Tato skupina se v implementaci vyskytuje pouze jednou.

Popis prvků:

0552 - Verze struktury segmentů
Hodnota '94W' definuje, že jsou použity služební bezpečnostní segmenty popsané v dokumentu UN/TRADE/WP.4/R.1026 a ISO/CD 9735 - 5.

0501 - Bezpečnostní funkce
Zpráva AUTACK má funkci neodmítnutí příjmu (hodnota '5').

0534 -Kontrolní reference
Tento prvek slouží jako jednoznačný klíč pro spojení skupin 1 (Security Header) a 3 (segment USY). Index se ale nepoužívá, neboť segment USY se odkazuje na Security Header přijaté zprávy. Hodnota link je '00' tak, aby nedocházelo ke kolizím s indexy z přijaté zprávy.

0541 - Rozsah zabezpečení
Hodnota '1' definuje, že hash přijaté zprávy je vypočítán z textu úvodních bezpečnostních segmentů (skupina 1 a 2) - od prvního písmene segmentu USH (tj. 'U') do oddělovače ukončujícího tyto segmenty včetně a z textu těla zprávy, který je bezprostředně připojen - od prvního znaku za oddělovačem ukončujícím úvodní bezpečnostní segmenty (tedy 'B' ze segmentu BGM) až do separátoru před koncovými bezpečnostními segmenty včetně. V případě jednoho podpisu to znamená, že se aplikuje hash funkce na souvislý text od 'U' segmentu USH až k ' ' ' před segmentem UST.
Tento prvek kopíruje hodnotu z přijaté zprávy není nutné jej tedy uvádět.

0503 - Typ odpovědi
Prvek je vynechán (zprávy AUTACK se již nesmí potvrzovat zprávou AUTACK - možnost vzniku cyklu).

0505 - Filtr (funkce)
Určuje typ funkce, která je použita pro filtrování binárních dat, která jsou výsledkem hashingu přijaté zprávy, před jejich zápisem do zprávy AUTACK (do prvku S508:0560 v segmentu USY, skupina 3).
Pro filtrování je možné využít buď hexadecimální filtr, nebo filtr definovaný v ISO 9735-5 (též v R.1026) tzv. UNO-A filtr, oba plně vyhovují UN/EDIFACT syntaktické úrovni A (jsou tedy universální). Vybraný filtr se potom používá na všechna binární data ve zprávě AUTACK.
Hexadecimální filtr reprezentuje jeden byte dvojicí znaků ('0' - '9', 'A' -'F'), první znak reprezentuje vrchní 4 bity, druhý spodní. V hexadecimálním zápisu představují levé znaky významnější byty. Nevýznamné nuly zleva mohou být vynechány.
Kód filter má následující hodnoty:
'2' - hexadecimální filtr

'5' - UNO-A filtr
Tento prvek kopíruje hodnotu z přijaté zprávy není nutné jej tedy uvádět.

0507 - Kódování znaků
Určuje kódování znaků přijaté EDIFACT zprávy před aplikací hash funkce. Zde je použito 8 bitové ASCII (hodnota '2').
Tento prvek kopíruje hodnotu z přijaté zprávy není nutné jej tedy uvádět.

0509 - Role podepisující strany
Strana je původcem zprávy AUTACK (hodnota '1')

S500 - Identifikace strany (první opakování)
S500 - Identifikace strany (druhé opakování)
0516 - Referenční číslo
S501 - Datum a čas
Prvky jsou vynechány.

SKUPINA 1 (M, 1)SEGMENT USA (O, 1) 1)

S.Prv. *S502*	**Prvek**	**P.** *M*	**Formát**	**Význam** *Bezp. algoritmus*	**Obsah**	**Komentář** *Algoritmus pro hash přijmuté zprávy*
S502	0523	M	an..3	Použití algoritmu - kód	'1'	Algoritmus je použit pro hashing zprávy
S502	0525	C	an..3	Operační mód - kód	'0'	Pro daný algoritmus nemá význam
S502	0533	O	an..3	Seznam operačních módů	'1'	Seznam definovaný UN/EDIFACT SJWG
S502	0527	C	an..3	Algoritmus - kód	'6'	Algoritmus MD5 (Rivest, Dusse - RSA Security Inc., 1991)
S502	0529	O	an..3	Seznam algoritmů	'1'	Seznam definovaný UN/EDIFACT SJWG
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*

Tento segment je kopírován ze Security Header přijaté zprávy, není tedy třeba jej uvádět, původci zprávy jsou jeho prvky implicitně známy.

Popis prvků:

S502 - Bezpečnostní algoritmus
Prvek popisuje uživatelův algoritmus použitý na hashing přijaté zprávy pro vytvoření otisku zprávy, který je potom uveden v segmentu USY.

S502:0523 - Použití algoritmu
viz tabulka

S502:0525 - Operační mód
viz tabulka

S502:0533 - Seznam operačních módů
Prvek definuje použitý seznam operačních módů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S502:0527 - Algoritmus
Prvek definuje použitý algoritmus. Podrobná specifikace algoritmu a jeho parametrů je v kapitole Parametry použitých kryptografických algoritmů.

S502:0529 - Seznam algoritmů
Prvek definuje použitý seznam algoritmů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S503 - Parametry algoritmu
Tyto prvky nejsou využity, algoritmus MD5 nepotřebuje žádné vstupní parametry.

SEGMENT USB (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0503	M	an..3	Typ odpovědi - kód	'1'	Zpráva nemá být potvrzena zprávou AUTACK
S501		*C*		*Datum a čas*		*Datum a čas vytvoření zprávy AUTACK*
S501	0517	M	an..3	Kvalifikátor datumu a času	'1'	Časová značka
S501	0338	C	n..8	Datum	date	date= datum, formát YYYYMMDD
S501	0314	C	n..15	Čas	time	time= čas, formát HHMMSS
S501	0336	O	n4	UTC offset (odchylka času)	offset	offset = '0100' - odchylka od UTC je + 1 hod (zimní čas) offset = '0200' - odchylka od UTC je + 2 hod (letní čas)

S002		*C*		*Odesílatel soub. výměny*		*Identifikace odesílatele zprávy AUTACK*
S002	0004	M	an..35	Identifikace odesílatele	send	send = odesílatel (dle ident. prvku segmentu UNB)
S002	0007	O	an..4	Kvalifikátor identifikace	qual_s	qual_s = kopie z segmentu UNB (pokud využito)
S002	0008	O	an..35	Identifikace odesílatele - 2 úroveň		Vynecháno
S002	0040	O	an..35	Identifikace odesílatele - 3 úroveň		Vynecháno
S003		*C*		*Příjemce soub. výměny*		*Identifikace příjemce zprávy AUTACK*
S003	0010	M	an..35	Identifikace příjemce	rec	rec = příjemce (dle ident. prvku segmentu UNB)
S003	0007	O	an..4	Kvalifikátor identifikace	qual_r	qual_r = kopie z segmentu UNB (pokud využito)
S003	0014	O	an..35	Identifikace příjemce - 2 úroveň		Vynecháno
S003	0044	O	an..35	Identifikace příjemce - 3 úroveň		Vynecháno

Popis prvků:

0503 - Typ odpovědi
Tento prvek určuje, že příjem zprávy AUTACK se již nesmí potvrzovat zprávou AUTACK (hodnota '1') - možnost vzniku cyklu.

S501 - Datum a čas
Tento prvek obsahuje datum a čas vytvoření zprávy AUTACK.

S501:0517 - Kvalifikátor datumu a času
viz tabulka

S501:0338 - Datum
Hodnota date musí mít předepsaný formát YYYYMMDD (např. 19950403).

S501:0314 - Čas
Hodnota time musí mít předepsaný formát HHMMSS (např. 182033). Hodnota time představuje běžný čas používaný v České republice.

S501:0336 - UTC offset
Tento prvek slouží pro rozlišení letního a zimního času. Hodnota offset udává odchylku lokálního času od standardního světového času, to znamená pro zimní čas + 1 hodina (hodnota '0100') a pro letní čas + 2 hodiny (hodnota '0200').

S002 - Odesílatel souboru výměny
Tento prvek obsahuje identifikaci odesílatele zprávy AUTACK. Údaje jsou převzaty z hlavičky souboru výměny, ve kterém je AUTACK odesílán (nebo ze souboru výměny, ve kterém byla referovaná zpráva, kdy příjemce zprávy je odesílatel AUTACKu).

S002:0004 - Identifikace odesílatele
Prvek obsahuje ID aplikace odesílatele zprávy. Hodnota send je okopírována z prvku S002:0004 ze segmentu UNB odesílaného souboru výměny (nebo prvku S003:0010 UNB přijatého souboru).

S002:0007 - Kvalifikátor identifikace
Pokud je hodnota qual_s uvedena je okopírována z prvku S002:0007 ze segmentu UNB odesílaného souboru výměny (nebo prvku S003: 0007 UNB přijatého souboru).

S002:0008 - Identifikace odesílatele - 2 úroveň
S002:0040 - Identifikace odesílatele - 3 úroveň
Prvky jsou vynechány.

S003 - Příjemce souboru výměny
Tento prvek obsahuje ID aplikace příjemce zprávy AUTACK. Údaje jsou převzaty z hlavičky souboru výměny, ve kterém je AUTACK odesílán (nebo ze souboru výměny, ve kterém je referovaná zpráva, kdy odesílatel zprávy je příjemce AUTACKu).

S003:0010 - Identifikace příjemce
Prvek obsahuje ID příjemce zprávy. Hodnota rec je okopírována z prvku S003:0010 ze segmentu UNB odesílaného souboru výměny (nebo prvku S002:0004 UNB přijatého souboru).

S003:0007 - Kvalifikátor identifikace
Pokud je hodnota qual_r uvedena je okopírována z prvku S003:0007 ze segmentu UNB odesílaného souboru výměny (nebo prvku S002:0007 UNB přijatého souboru).
.

S003:0014 - Identifikace příjemce - 2 úroveň
S003:0044 - Identifikace příjemce - 3 úroveň
Prvky jsou vynechány.

SKUPINA 3 (M, 1 - 9999) SEGMENT USX (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0020	M	an..14	Ref. číslo soub. výměny	itc_ref	itc_ref = reference přijaté výměny (hodnota z UNB)
S002		*O*		*Odesílatel soub. výměny*		*Vynecháno*
	0048	O	an..14	Ref. číslo skupiny		Vynecháno
S006		*O*		*Aplikační identifikace odesílatele*		*Vynecháno*
S007		*O*		*Aplikační identifikace příjemce*		*Vynecháno*
	0062	C	an..14	Ref. číslo zprávy	msg_ref	msg_ref = reference přijaté zprávy (hodnota z UNH)
	0800	O	an..14	Ref. číslo balíku		Vynecháno
S501		*C*		*Datum a čas*		*Datum a čas vytvoření referovaných zpráv*
S501	0517	M	an..3	Kvalifikátor datumu a času	'5'	Datum a čas vytvoření referované zprávy
S501	0338	C	n..8	Datum	date	date= datum, formát YYYYMMDD
S501	0314	C	n..15	Čas	time	time= čas, formát HHMMSS
S501	0336	O	n4	UTC offset (odchylka času)	offset	offset = '0100' - odchylka od UTC je + 1 hod (zimní čas) offset = '0200' - odchylka od UTC je + 2 hod (letní čas)
S509		*O*		*Bezpečnostní reference*		*Vynecháno*

Skupina segmentů 3 (USX, USY) obsahuje reference přijaté zprávy a výsledky příjmu zprávy. Tato skupina se v rámci AUTACK opakuje pro každou referovanou zprávu.

Popis prvků:

0020 - Referenční číslo souboru výměny
Hodnota itc_ref obsahuje hodnotu prvku 0020 ze segmentu UNB souboru výměny, ve kterém byla obsažena referovaná zpráva.

S002 - Odesílatel souboru výměny
0048 - Referenční číslo skupiny
S006 - Aplikační identifikace odesílatele
S007 - Aplikační identifikace příjemce
Prvky jsou vynechány.

0062 - Referenční číslo zprávy
Hodnota msg_ref obsahuje hodnotu prvku 0062 ze segmentu UNH referované zprávy.

0800 - Referenční číslo balíku
Prvek je vynechán.

S501 - Datum a čas
Tento prvek obsahuje datum a čas vytvoření referované zprávy. Jako čas vytvoření zprávy je brán čas vytvoření digitálního podpisu. Údaje do tohoto prvku jsou převzaty z prvku S501 v segmentu USH referované zprávy.

S501:0517 - Kvalifikátor datumu a času
viz tabulka

S501:0338 - Datum
Hodnota date musí mít předepsaný formát YYYYMMDD (např. 19950403).

S501:0314 - Čas
Hodnota time musí mít předepsaný formát HHMMSS (např. 182033). Hodnota time představuje běžný čas používaný v České republice.

S501:0336 - UTC offset
Tento prvek slouží pro rozlišení letního a zimního času. Hodnota offset udává odchylku lokálního času od standardního světového času, to znamená pro zimní čas + 1 hodina (hodnota '0100') a pro letní čas + 2 hodiny (hodnota '0200').

S509 - Bezpečnostní reference
Prvek je vynechán.

SKUPINA 3 (M, 1-9999) , SEGMENT USY (M, 1-9)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0534	M	an..14	Kontrolní reference	link	link = index z USH/UST přijaté zprávy
S508		*C*		*Výsledek bezp. funkce*		*Výsledek příjmu zprávy*
S508 S508	0560 0560	M O	an..256 an..256	Výsledná hodnota Výsledná hodnota	chck_val	chck_val = hash přijaté zprávy Vynecháno
	0571	C	an..3	Chyba zabezpečení - kód	err_code	err_code = kód chyby zjištěné při příjmu zprávy

Popis prvků:

0534 - Kontrolní reference
Prvek se odkazuje na segmenty USH a UST z referované zprávy, která je potvrzována. Hodnota link je potom převzata z prvku 0534 v příslušném segmentu USH referované zprávy.

S508 - Výsledek bezpečnostní funkce
Obsahuje otisk referované zprávy.

S508:0560 - Výsledná hodnota (první výskyt)
Hodnota chck_val je otisk referované zprávy ve filtrovaném tvaru (viz prvek 0505), vypočtený stejným algoritmem, jaký byl použit při kontrole referované zprávy.

S508:0560 - Výsledná hodnota (druhý výskyt)
Prvek není použit.

0571 - Chyba zabezpečení
Tento prvek obsahuje kód chyby zjištěné při kontrole referované zprávy.
Pokud prvek není uveden předpokládá se potvrzení příjmu zprávy.
Hodnoty err_code jsou:
'1' - chyba při ověřování autentizace zprávy
'2' - chyba při ověřování autentizace certifikátu (potřebného pro ověření podpisu)
'3' - k certifikátu není dostupný certifikát CA (nekompletní certifikační cesta)
'4' - asymetrický šifrovací algoritmus není podporován
'5' - hash funkce není podporována
'6' - certifikát má prošlou platnost
'7' - certifikát ještě nezačal platit
'8' - certifikát byl zrušen
'9' - neznámý certifikát (posláno pouze referenční číslo a není v lokální databázi)
'10' - špatná časová značka (větší než aktuální čas)
'11' - špatná syntaxe bezpečnostních segmentů.
'12' - špatný otisk zprávy
'13' - zabezpečení zprávy neodpovídá požadovanému
'14' - chyba při dešifrování zprávy
'999' - nespecifikovaná chyba

SEGMENT UNT (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0074	M	n..6	Počet segmentů	seg_no	seg_no = počet segmentů ve zprávě
	0062	M	an..14	Ref. číslo zprávy	ref_no	ref_no = ref. číslo, jednoznačné

Segment UNT je standardní služební segment, který využívají všechny UN/EDIFACT zprávy, jeho použití se řídí standardními pravidly UN/EDIFACT.

Příklad zprávy AUTACK

Příklad souboru výměny se zprávou AUTACK, která potvrzuje příjem zprávy z příkladu v kapitole Implementace digitálního podpisu – Příklad podepsané zprávy:

Segmenty	**Komentář**
UNB+UNOA:1+CNBASUD+BANK+960521:2007+AUTACK0028'	Hlavička souboru výměny, jedná se o soubor výměny od aplikace CNBASUD pro aplikaci BANK .
UNH+120000000637+AUTACK:D:94A:UN'	Hlavička zprávy, jedná se o zprávu AUTACK, její referenční číslo je 120000000637.
USH+94W+1+01+1+1+2+2+1+++120000000637+1:1 9960521:200742:0200' USA+1:0:1:6:1' USC+CATEST000000022'	Úvodní bezpečnostní segmenty, definují digitální podpis zprávy AUTACK, který je proveden standardním způsobem. USH segment definuje především typ funkce (digitální podpis), referenci podpisu (01), zpráva nemá být potvrzena (kód 1), použitou filtr funkci (hexadecimální), bezpečnou kopii ref. čísla zprávy, timestamp vytvoření podpisu. Segment USA definuje použitou hash funkci (MD5). Segment USC obsahuje odkaz na certifikát, který musí být použit při kontrole podpisu.
USH+94W+5+00'	Segment USH definuje funkci zprávy AUTACK, tj. neodmítnutí příjmu (kód 5).
USB+1+1:19960521:200740:0200+CNBASUD+BANK'	USB segment obsahuje datum a čas vytvoření zprávy AUTACK a odesílatele (CNBASUD) a příjemce (BANK) zprávy AUTACK.
USX+000010033+++++236++5:19960521:200246:0200'	Segment USX obsahuje referenci na potvrzovanou zprávu: číslo souboru výměny (000010033), číslo zprávy (236) a datum a čas vytvoření podpisu zprávy.
USY+01+A4D37E33EB795A9B115BA36646C01F3A'	Segment USY obsahuje referenci podpisu přijaté zprávy (01) a filtrovaný hash kód přijaté zprávy.
UST+01' USR+58AFDF12B0EC9CC398C57C67F4268C49FBC0CD7F539766D0DE020A6808A9CEAA5B8806A26B8DC68B4DADBA46F87D977EAD07C8FF349843F849B4D3D7E0096209C316ABD943315C4436889A9F0100D2814F6AEC185BA1C7F6589CD5B77B3A58840BAB458FEC74A2E31AF86B00DA12D3CAC506B5A2D9E90BDB17833CC9FE2EF42F'	Koncové bezpečnostní segmenty, obsahují digitální podpis zprávy AUTACK, který je proveden standardním způsobem. Segment UST svazuje koncové bezpečnostní segmenty s úvodními pomocí reference podpisu (01). Segment USR obsahuje samotný digitální podpis zprávy ve filtrované podobě.
UNT+11+120000000637'	Patička zprávy, zpráva obsahuje 11 segmentů (včetně služebních).
UNZ+1+ AUTACK0028'	Patička souboru výměny, soubor výměny obsahuje 1 zprávu.

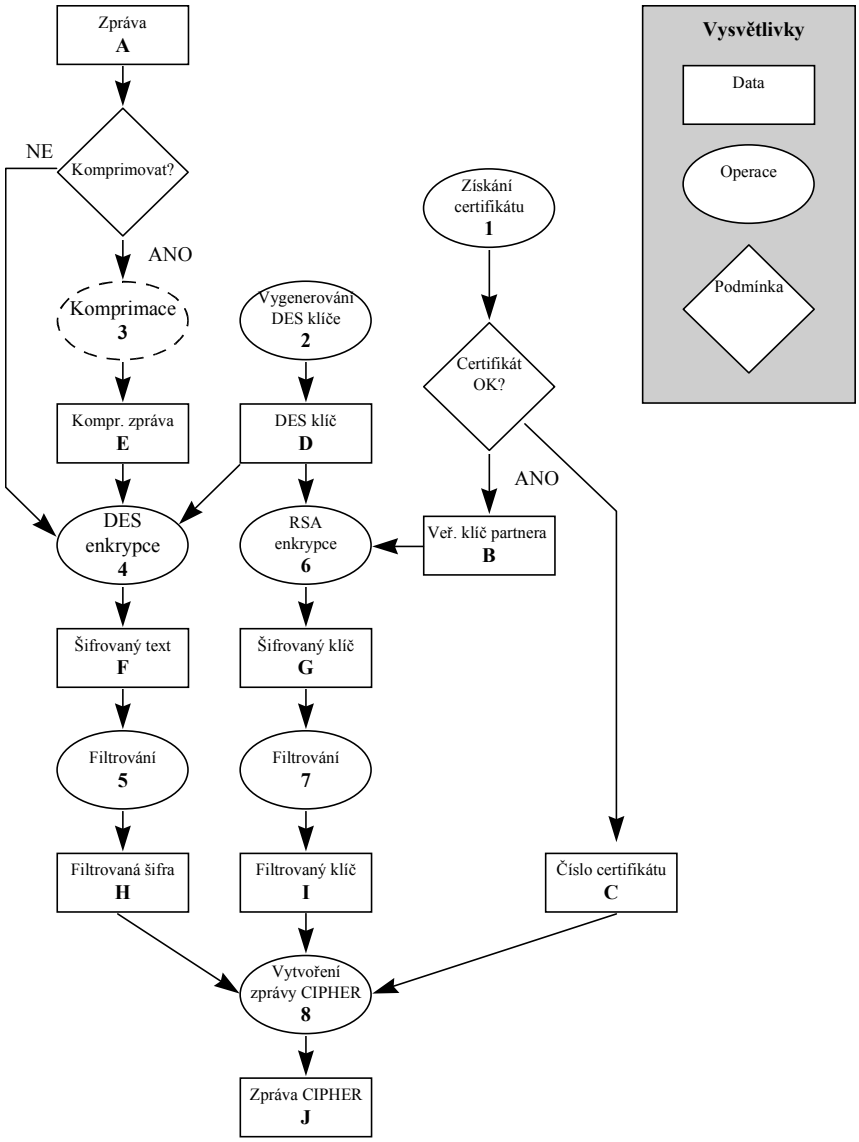
Implementace zprávy CIPHER

Princip použití zprávy CIPHER

Zpráva CIPHER slouží pro šifrování přenášených UN/EDIFACT zpráv. Zpráva CIPHER může obsahovat zašifrovaný text libovolné EDIFACT zprávy a je umístěna v souboru výměny místo zprávy původní. Při příjmu je potom opět ze zprávy CIPHER dešifrována zpráva původní a nahradí v souboru výměny CIPHER.

Na následujícím obrázku je uvedeno schéma zašifrování jedné zprávy:

OBR. 7 - Schéma vytvoření zprávy CIPHER

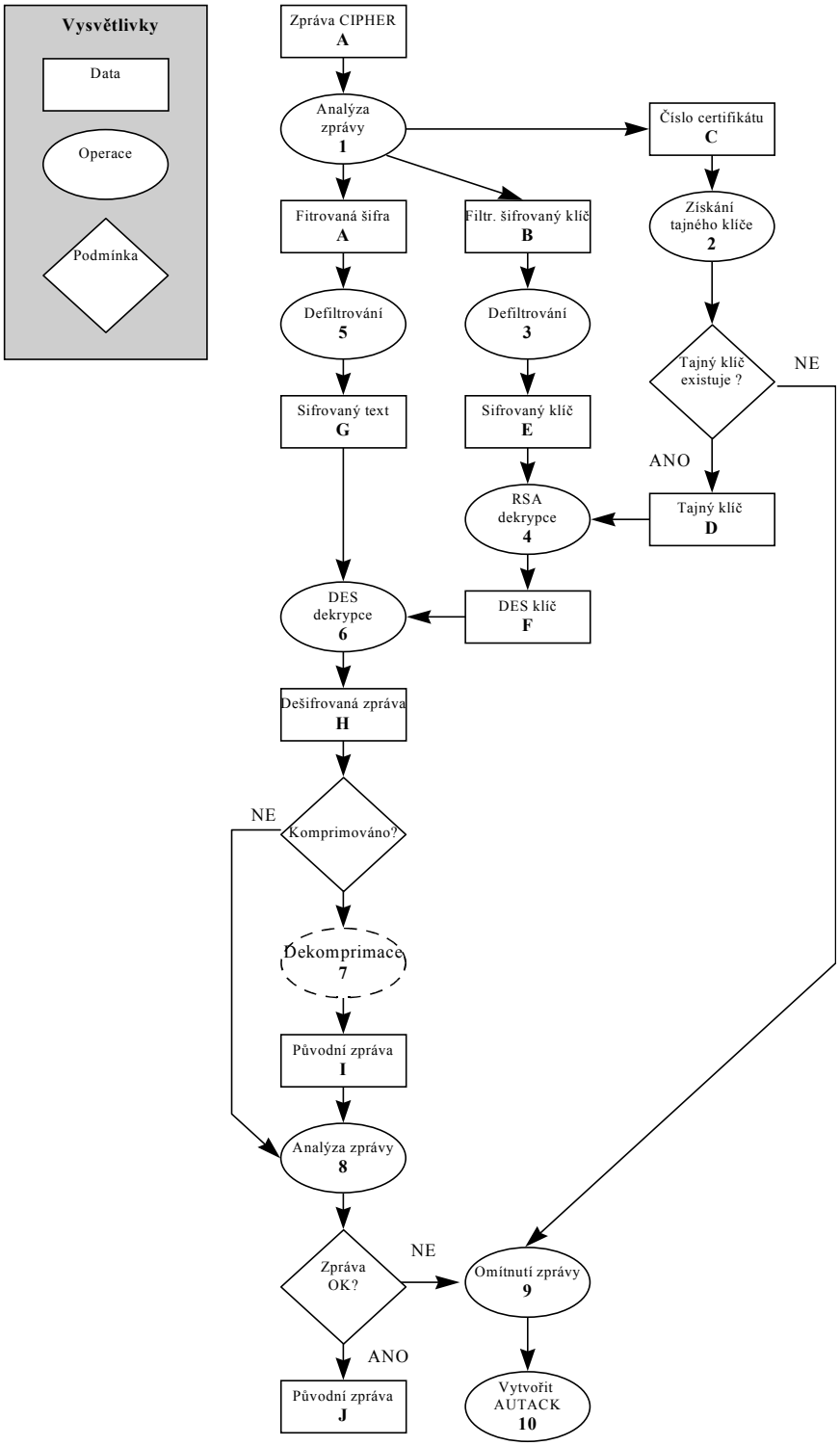


Pro enkrypci zprávy a vytvoření zprávy CIPHER platí následující postup následující postup:

1. Je získán certifikát partnera obsahující veřejný klíč partnera [B], který je určen pro šifrování zpráv, a je také z certifikátu získáno jeho referenční číslo [C]. Pokud není certifikát platný nebo jej nelze získat, nemůže být zpráva šifrována.
2. Je vygenerován DES klíč [D], tento klíč musí být náhodný a může být použit pouze pro zašifrování této jedné zprávy.
3. Text původní zprávy [A] může být komprimován zvoleným algoritmem. Tato možnost nebude u aplikace SÚD využita.
4. Celá původní zpráva [A] nebo komprimovaná zpráva [E] je zašifrována algoritmem DES s využitím vygenerovaného DES klíče [D].
5. Výsledný šifrovaný text [F] je filtrován do textové podoby, tak aby mohl být přenášen v UN/EDIFACT zprávě.
6. DES klíč je zašifrován RSA algoritmem veřejným klíčem partnera [B] tak, že první byte (index 0) odpovídá nejvyššímu řádu čísla.
7. Šifrovaný DES klíč [G] je filtrován do textové podoby, tak aby mohl být přenášen v UN/EDIFACT zprávě.
8. Je vytvořena zpráva CIPHER, která obsahuje filtrovanou šifrovanou zprávu [H], filtrovaný šifrovaný DES klíč [I], číslo certifikátu, který byl použit pro šifrování DES klíče [C], a další standardní údaje (viz. Syntaktická pravidla a formální pravidla pro zprávu CIPHER).

Na následujícím obrázku je uvedeno schéma dešifrování zprávy CIPHER a získání původní zprávy:

OBR. 8 - Schéma získání původní zprávy



Při příjmu zprávy CIPHER je získána původní zpráva následujícím postupem:

1. Zpráva CIPHER [A] je analyzována a ze zprávy jsou získány potřebné údaje, především filtrovaný šifrovaný text původní zprávy [B], filtrovaný šifrovaný DES klíč [C] a číslo certifikátu použitého pro šifrování DES klíče [D].
2. Podle čísla certifikátu [D] se získá potřebný tajný klíč uživatele [E] pro dešifrování DES klíče (tj. klíč tvořící pár s veřejným klíčem z certifikátu).
3. Filtrovaný DES klíč [C] je defiltrován do binárního tvaru [F].
4. Šifrovaný DES klíč je dešifrován algoritmem RSA za pomoci tajného klíče uživatele [E].
5. Filtrovaný šifrovaný text původní zprávy [B] je defiltrován do binárního tvaru [H].
6. Šifrovaný text původní zprávy [H] je dešifrován algoritmem DES s využitím DES klíče [G] získaného ze zprávy.
7. Pokud byl text původní zprávy [I] před šifrováním komprimován, je nyní dekomprimován.
8. Původní zpráva [J] je zkontrolována, zda byla dešifrována korektně (musí odpovídat UN/EDIFACT syntaxi).
9. Pokud zpráva nebyla korektně dešifrována nebo nelze získat tajný klíč pro její dešifrování, musí být zpráva CIPHER odmítnuta a nemůže být dále zpracována.
10. Pokud zpráva nebyla korektně dešifrována nebo nelze získat tajný klíč pro její dešifrování, vytvoří příjemce chybovou zprávu AUTACK, kterou pošle odesílateli zprávy CIPHER (viz kapitola Implementace zprávy AUTACK).

Syntaktická pravidla a formální pravidla pro zprávu CIPHER

Zpráva CIPHER je implementována podle dokumentu "Cipher Text Message- EDIFACT Message Implementation Guidelines", UN/ECE/SJWG a dokumentů ISO/CD 9735-5,6.

Zpráva CIPHER obsahuje šifrovaný text celé UN/EDIFACT zprávy, to znamená, že vstupem do šifrovacího algoritmu je text (jako posloupnost bytů) od prvního znaku segmentu UNH (tj. ´U´) původní zprávy až do koncového oddělovače segmentu UNT (tj. ' ' ') původní zprávy včetně. Pokud je použita kompresní funkce, vstupuje tento text nejprve do kompresního algoritmu a teprve výsledek komprese je vstupem do šifrovacího algoritmu.

Pokud má být text před šifrováním komprimován, je specifikována komprimační funkce v prvku 0519 segmentu USH (pro toto řešení nebude využito, tj. nebude se tento prvek vyskytovat).

Šifrovaný text a šifrovaný DES klíč jsou filtrovány stejným algoritmem, který je specifikován v prvku 0505 segmentu USH.

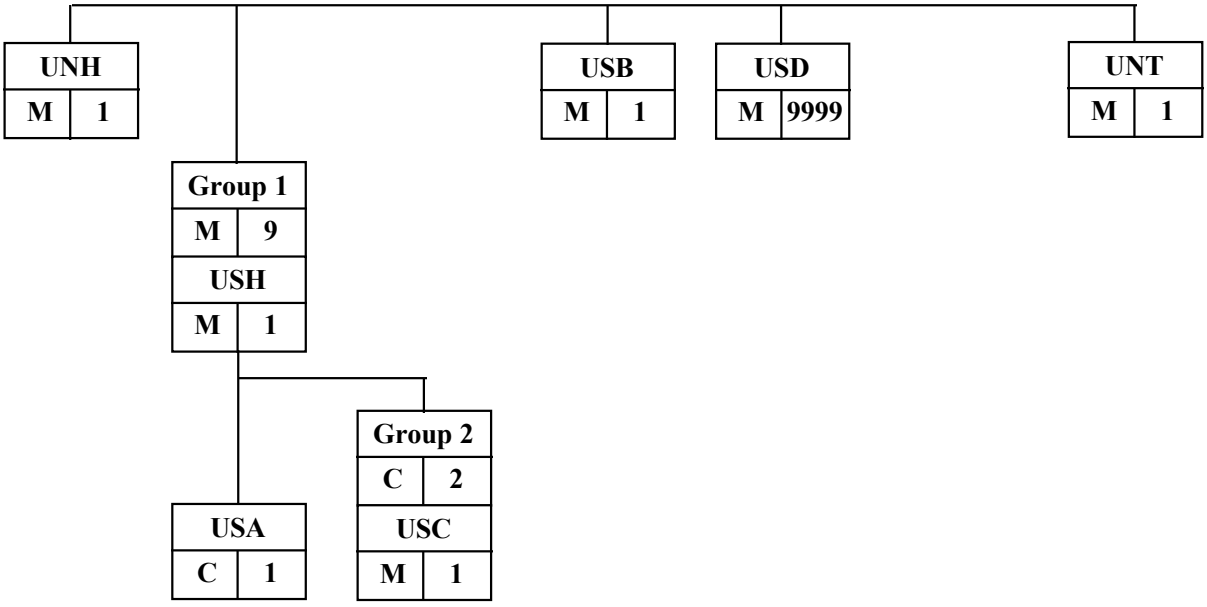
Výsledný šifrovaný text je filtrován do textové podoby a potom je rozdělen na bloky velké 512 bytů (poslední blok může být menší, podle toho kolik dat zbude) a každý blok je potom vložen do segmentu USD v těle zprávy CIPHER (postupuje se zleva, tj. první 512

bytový blok zleva - první opakování USD atd.). Obdobným způsobem je zpětně skládán šifrovaný text z USD segmentů (tj. postupuje se zleva).

Detailní parametry algoritmu DES jsou uvedeny v kapitole Parametry použitých kryptografických funkcí.

Pokud se zpráva současně zabezpečuje pomocí digitálního podpisu a šifruje pomocí zprávy CIPHER, musí nejprve proběhnout digitální podpis zprávy, teprve potom může být zpráva zašifrována.

OBR. 9 Struktura zprávy CIPHER



Význam a popis bezpečnostních segmentů je v tab. 5.

TAB. 5 Popis bezpečnostních segmentů
M/C - povinný (M), použitý nepovinný (C), běžně nepoužívaný (O) segment (skupina)
Op. - počet opakování, v závorce je uveden maximální počet povolený standardem. V () je uvedeno opakování, které nebude využito, v [] jsou uvedeny opakování, které lze využít v jiných implementacích.

SKUPINA SEGMENT	M/C	Op.	POPIS
1	M	1(9)	Tato skupina segmentů slouží k identifikaci použitých bezpečnostních funkcí.
USH	M	1	Definuje parametry pro funkci důvěrnost zprávy
USA	C	1	Obsahuje specifikaci šifrovacího algoritmu a také šifrovaný symetrický klíč
2	C	1(2)	Skupina segmentů 2 identifikuje použitý certifikát příjemce zprávy
USC	M	1	Obsahuje číslo certifikátu, který byl použit pro zašifrování symetrického klíče, ev. identifikaci vlastníka certifikátu.
USB	M	1	Úvodní segment těla ,obsahuje časovou značku.
USD	M	9999	Obsahuje šifrovanou zprávu.

Podrobný popis jednotlivých segmentů a jejich struktury je v tab. 6

TAB. 6 Struktura bezpečnostních segmentů

S.Prv. - Číslo složeného prvku v UN/EDIFACT Standard Directory
Prvek - Číslo prvku v UN/EDIFACT Standard Directory
P. - povinný (M), použitý nepovinný (C), běžně nepoužívaný (O) segment, prvek
Formát - specifikace formátu dle konvencí UN/EDIFACT
Obsah - v ' ' jsou uváděny konstanty, textové identifikátory odkazují na proměnné hodnoty dodávané bezpečnostní aplikací

SEGMENT UNH (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0062	M	an..14	Ref. číslo zprávy	ref_no	ref_no = ref. číslo, stejné jako u originální zprávy
S009		*M*		*Identifikátor zprávy*		*Identifikuje typ UN/EDIFACT zprávy*
S009	0065	M	an..6	Typ zprávy	'CIPHER'	
S009	0052	M	an..3	Verze zprávy	'1'	
S009	0054	M	an..3	Číslo verze	'932'	
S009	0051	M	an..2	Odpovědná agentura	'UN'	
S009	0057	O	an..6	Speciální kód		Vynecháno
	0068	O	an..35	Společná reference		Vynecháno
S010		*O*		*Stav přenosu*		*Vynecháno*

Segment UNH je standardní služební segment, který využívají všechny UN/EDIFACT zprávy,
jeho použití se řídí standardními pravidly UN/EDIFACT. Speciální přístup vyžaduje pouze prvek 0062.

0062 - Referenční číslo zprávy
Referenční číslo zprávy (ref_no) je stejné jako u původní zprávy.

SKUPINA 1 (M,1) SEGMENT USH (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0552	M	an..3	Verze struktury segmentů	'94W'	Verze z roku 1994
	0501	M	an..3	Bezp. funkce - kód	'4'	Utajení obsahu
	0534	M	an..14	Kontrolní reference	'00'	Číslo 00 - aby nebyla kolize s dig. podpisem
	0541	O	an..3	Rozsah zabezpečení - kód		Vynecháno
	0503	O	an..3	Typ odpovědi - kód		Vynecháno
	0505	C	an..3	Filtr (funkce) - kód	filter	Filtr pro binární data
	0507	C	an..3	Kódování znaků -kód	'2'	ASCII 8 bitů 1)
	0509	C	an..3	Role strany - kód	'1'	Původce dokumentu
S500		*O*		*Identifikace strany*		*Vynecháno*
S500		*O*		*Identifikace strany*		*Vynecháno*
	0516	O	an..35	Referenční číslo	ref_no	Vynecháno
S501		*O*		*Datum a čas*		*Vynecháno*
	0519	O	an..3	Kompresní funkce - kód	comp	comp = kód použité kompresní funkce

Skupina 1 obsahuje údaje o funkci zprávy CIPHER a parametry šifrovacího algoritmu, včetně zašifrovaného DES klíče. Tato skupina se v implementaci vyskytuje pouze jednou.

Popis prvků:

0552 - Verze struktury segmentů
Hodnota '94W' definuje, že jsou použity služební bezpečnostní segmenty popsané v dokumentu UN/TRADE/WP.4/R.1026 a ISO/CD 9735 - 5.

0501 - Bezpečnostní funkce
Zpráva CIPHER má funkci utajení obsahu (kód '4').

0534 -Kontrolní reference
link je '00' tak, aby bylo zřejmé, že se neváže k žádnému Security Trailer.

0541 - Rozsah zabezpečení
Prvek je vynechán.

0503 - Typ odpovědi
Prvek je vynechán.

0505 - Filtr (funkce)
Určuje typ funkce, která je použita pro filtrování binárních dat, která jsou výsledkem šifrování zprávy , před jejich zápisem do zprávy CIPHER (do segmentu USD).
Pro filtrování je možné využít buď hexadecimální filtr, nebo filtr definovaný v ISO 9735-5 (též v R.1026) tzv. UNO-A filtr, oba plně vyhovují UN/EDIFACT syntaktické úrovni A (jsou tedy universální). Vybraný filtr se potom používá na všechna binární data ve zprávě CIPHER.
Hexadecimální filtr reprezentuje jeden byte dvojicí znaků ('0' - '9', 'A' -'F'), první znak reprezentuje vrchní 4 bity, druhý spodní. V hexadecimálním zápisu představují levé znaky významnější byty. Nevýznamné nuly zleva mohou být vynechány.
Kód filter má následující hodnoty:
'2' - hexadecimální filtr
'5' - UNO-A filtr

0507 - Kódování znaků
Určuje kódování znaků přijaté EDIFACT zprávy před aplikací hash funkce. Zde je použito 8 bitové ASCII (hodnota '2').

0509 - Role podepisující strany
Strana je původcem zprávy CIPHER (hodnota '1')

S500 - Identifikace strany (první opakování)
S500 - Identifikace strany (druhé opakování)
0516 - Referenční číslo
S501 - Datum a čas
Prvky jsou vynechány.

0519 - Kompresní funkce - kód
Tento prvek udává, zda byl text před šifrováním komprimován a pokud ano specifikuje použitou komprimační funkci. Pro současnou aplikaci se nepočítá s implementací komprimační funkce, je možné její pozdější nasazení.
Pokud prvek není uveden, nebyla komprese uplatněna.
Hodnoty comp nejsou zatím definovány.

SKUPINA 1 (M, 1)SEGMENT USA (C, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
S502		*M*		*Bezp. algoritmus*		*Algoritmus pro hash přijmuté zprávy*
S502	0523	M	an..3	Použití algoritmu - kód	'2'	Symetrický algoritmus pro šifrování zprávy
S502	0525	C	an..3	Operační mód - kód	'2'	DES mód CBC - ISO 8372
S502	0533	O	an..3	Seznam operačních módů	'1'	Seznam definovaný UN/EDIFACT SJWG
S502	0527	C	an..3	Algoritmus - kód	'1'	Algoritmus DES - FIPS Pubs 46
S502	0529	O	an..3	Seznam algoritmů	'1'	Seznam definovaný UN/EDIFACT SJWG
S503		*C*		*Parametry algoritmu*		*Šifrovaný DES klíč*
S503	0532	C	an..512	Hodnota parametru	DES_key	DES_key = šifrovaný DES klíč
S503	0531	C	an..3	Kvalifikátor param. - kód	'6'	Symetrický klíč šifrovaný veřejným klíčem
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*
S503		*O*		*Parametry algoritmu*		*Vynecháno - pro daný algoritmus nemá význam*

Popis prvků:

S502 - Bezpečnostní algoritmus
Prvek popisuje uživatelův symetrický šifrovací algoritmus (DES) používaný pro šifrování zpráv odesílaných uživatelem (kód 0523 = '2').

S502:0523 - Použití algoritmu
viz tabulka

S502:0525 - Operační mód
viz tabulka

S502:0533 - Seznam operačních módů
Prvek definuje použitý seznam operačních módů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S502:0527 - Algoritmus
Prvek definuje použitý algoritmus. Podrobná specifikace algoritmu a jeho parametrů je definována v kapitole Parametry použitých kryptografických algoritmů.

S502:0529 - Seznam algoritmů
Prvek definuje použitý seznam algoritmů. V tomto případě je použit seznam definovaný v materiálu UN/TRADE/WP.4/R.1026 z roku 1994 (hodnota '1').

S503 - Parametry algoritmu (první výskyt)
Tento prvek obsahuje DES klíč zašifrovaný veřejným klíčem příjemce zprávy.

S503:0532 - Hodnota parametru
Hodnota DES_key je DES klíč zašifrovaný veřejným klíčem příjemce zprávy. Hodnota je uvedena filtrovaná (viz popis prvku 0505 v segmentu USH).

S503:0531 - Kvalifikátor parametru
viz tabulka

S503 - Parametry algoritmu (další výskyty)
Tyto prvky nejsou využity, pro použité schéma není třeba dalších parametrů.

SKUPINA 2 (C, 1) SEGMENT USC (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0536	C	an..35	Ref. číslo certifikátu	ref_num	ref_num= referenční číslo certifikátu - unikátní
S500		*O*		*Identifikace strany*		*Identifikace vlastníka certifikátu*
S500	0577	M	an..3	Kvalifikátor strany	'3'	Vlastník certifikátu
S500	0538	C	an..35	Jméno klíče	key1	key1= číslo (jméno) certifikovaného klíče
S500	0511	C	an..17	ID strany	EDI_ID	EDI_ID= EDI identifikace organizace vlastníka klíče
S500	0513	O	an..3	Použitý seznam stran	'1'	Kód seznamu partnerů (EDI aplikací)
S500	0515	O	an..3	Agentura udržující seznam	'CNB'	Kód agenturry udržující seznam
S500	0586	O	an..35	Jméno strany	org_name1	org_name1= jméno organizace
S500	0586	O	an..35	Jméno strany	org_dep1	org_dep1= oddělení (pobočka) v organizaci
S500	0586	O	an..35	Jméno strany	org_pers1	org_pers1= odpovědný pracovník
S500		*O*		*Identifikace strany*		*Vynecháno*
	0544	O	an..3	Verze formátu certifikátu		Vynecháno
	0505	O	an..3	Filtr (funkce) - kód		Vynecháno
	0507	O	an..3	Kódování znaků -kód		Vynecháno
	0543	O	an..3	Výběr znaků - kód		Vynecháno
	0546	O	an..35	Úroveň práv		Vynecháno
S505		*O*		*Oddělovače*		*Vynecháno*
S505		*O*		*Oddělovače*		*Vynecháno*
S505		*O*		*Oddělovače*		*Vynecháno*
S505		*O*		*Oddělovače*		*Vynecháno*
S501		*O*		*Datum a čas*		*Vynecháno*
S501		*O*		*Datum a čas*		*Vynecháno*

S501		*O*		*Datum a čas*		*Vynecháno*
	0567	O	an..3	Bezpečnostní status, kód		Vynecháno

Segment USC identifikuje certifikát, který byl použit (resp. veřejný klíč v něm obsažený) pro zašifrovaní DES klíče obsaženého v segmentu USA. Jedná se tedy o certifikát klíče, který patří příjemci zprávy CIPHER. Certifikát je jednoznačně identifikován pomocí svého referenčního čísla.

Popis prvků

0536 - Referenční číslo certifikátu
Tento prvek obsahuje referenční číslo certifikátu.

S500 - Identifikace strany (první opakování)
Tento prvek může sloužit pro dodatečné specifikování příjemce. Jeho hodnoty musí odpovídat hodnotám uvedeným v certifikátu. Vzhledem k tomu, že referenční číslo certifikátu jednoznačně identifikuje certifikát i příjemce, nebude běžně využíván.

S500:0577 - Kvalifikátor strany
viz tabulka

S500:0538 - Jméno klíče
Obsahuje identifikaci uživatelova veřejného klíče obsaženého v certifikátu.

S500:0511 - ID strany
Obsahuje identifikaci organizace pro EDI. Hodnotu EDI_ID přiděluje EDIVAN.

S500:0513 - Použitý seznam stran
S500:0515 - Agentura udržující seznam
Pro současnou aplikaci se počítá pouze s jedním seznamem, hodnoty tedy nebudou uvedeny; hodnoty uvedené v tabulce jsou pokládány za defaultní. Jejich využití se předpokládá později, pokud bude více lokálních EDI aplikací.

S500:0586 Jméno strany
Určeno pro detailnější specifikaci strany

Ostatní prvky v segmentu USC jsou vynechány.

SEGMENT USB (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0503	M	an..3	Typ odpovědi - kód	'1'	Zpráva nemá být potvrzena zprávou AUTACK
S501		*C*		*Datum a čas*		*Datum a čas šifrování zprávy*
S501	0517	M	an..3	Kvalifikátor datumu a času	'1'	Časová značka
S501	0338	C	n..8	Datum	date	date= datum, formát YYYYMMDD
S501	0314	C	n..15	Čas	time	time= čas, formát HHMMSS
S501	0336	O	n4	UTC offset (odchylka času)	offset	offset = '0100' - odchylka od UTC je + 1 hod (zimní čas) offset = '0200' - odchylka od UTC je + 2 hod (letní čas)
S002		*O*		*Odesílatel soub. výměny*		*Vynecháno*
S003		*O*		*Příjemce soub. výměny*		*Vynecháno*

Popis prvků:

0503 - Typ odpovědi
Tento prvek určuje, že příjem zprávy CIPHER se nemá potvrzovat zprávou AUTACK (hodnota '1'). Eventuální potvrzení zprávy se totiž provádí až po dešifrování zprávy CIPHER, kdy se zpráva AUTACK vytvoří na původní zprávu, která je opatřena digitálním podpisem, podle požadavku uvedeném v prvku 0503 v segmentu USH (viz také kapitola Implementace zprávy AUTACK).

S501 - Datum a čas
Tento prvek obsahuje datum a čas vytvoření zprávy CIPHER.

S501:0517 - Kvalifikátor datumu a času
viz tabulka

S501:0338 - Datum
Hodnota date musí mít předepsaný formát YYYYMMDD (např. 19950403).

S501:0314 - Čas
Hodnota time musí mít předepsaný formát HHMMSS (např. 182033). Hodnota time představuje běžný čas používaný v České republice.

S501:0336 - UTC offset
Tento prvek slouží pro rozlišení letního a zimního času. Hodnota offset udává odchylku lokálního času od standardního světového času, to znamená pro zimní čas + 1 hodina (hodnota '0100') a pro letní čas + 2 hodiny (hodnota '0200').

S002 - Odesílatel souboru výměny
S003 - Příjemce souboru výměny
Prvky jsou vynechány.

SEGMENT USD (M, 9999)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0522	M	an..512	Zašifrovaný text	ciph_txt	ciph_txt = šifrovaný text, rozdělený na bloky, filtrovaný

Segment USD obsahuje přefiltrovaný šifrovaný text. Počet opakování segmentu je volen tak, aby byl pokryt celý text. Při rozdělování textu na 512 bloky a ukládání do USD segmentu se postupuje zleva.

Popis prvků:

0522 - Zašifrovaný text
Obsahuje 512 bytů (kromě posledního opakování) filtrovaného (funkcí specifikovanou v USH 0505) a šifrovaného textu původní zprávy.

SEGMENT UNT (M, 1)

S.Prv.	Prvek	P.	Formát	Význam	Obsah	Komentář
	0074	M	n..6	Počet segmentů	seg_no	seg_no = počet segmentů ve zprávě
	0062	M	an..14	Ref. číslo zprávy	ref_no	ref_no = ref. číslo, jednoznačné

Segment UNT je standardní služební segment, který využívají všechny UN/EDIFACT zprávy, jeho použití se řídí standardními pravidly UN/EDIFACT.

Příklad zprávy CIPHER

Příklad souboru výměny se zašifrovanou zprávou (jedná se o soubor výměny se zprávou GESMES z příkladu v kapitole Implementace digitálního podpisu – Příklad podepsané zprávy):

Segmenty	Komentář
UNB+UNOD:2+BANK+CNBASUD+960521:2002+0 00010033'	Hlavička souboru výměny, jedná se o soubor výměny od aplikace BANK pro aplikaci CNBASUD.
UNH+236+CIPHER:2:951:UN'	Hlavička zprávy, jedná se o zprávu CIPHER, její referenční číslo je 236.
USH+94W+4+00+++2+2+1	USH segment definuje funkci zprávy CIPHER (utajení dat) a použitý filtr pro šifrovaná data a šifrovaný DES klíč (hexadecimální).

USA+2:2:1:1:1+801D992110315F5A796AB70F1E8D 1A56EA4E9867EDDA55291D898E8062825C1A173 A7B0DA11F99D98D838E2C2D69FB3B6C8A21F2A A6875290D2F89EE7B61BEA9F808517EE2B0B9BB 73E8478DD0DD285673480DE9E2D0352BE0B16FF E57CDBD6029097F69B85E7F67126D2B5A87B819 A048A4E0139EFE8A08E4915B63EC7BE30B:6'	Segment USA definuje parametry šifrovacího algoritmu (DES mód CBC) a obsahuje filtrovaný šifrovaný DES klíč.
USC+CATEST000000022'	Segment USC obsahuje odkaz na certifikát, který byl použit pro zašifrování DES klíče.
USB+1+1:19960521:200249:0200	Segment USB obsahuje datum a čas vytvoření zprávy CIPHER.
USD+940CB4938F319A5E37E1F882E3CF5C7A938 B4C7269A5EE082B0D2F17BE4779E904E28E6F617 F2F75E755E560A7D9DB2E1F208EE41B1BB97F850 4B80B5F779B80542DF98C46F39561FE4F375C635D 010DE828F3B492615229E20212A91545DABA60BF 2E15FE1B89931C860E0C1DA5AC54EF5959F3CBF 051436B5254503C84163CD61D9CF7CE778B8D816 E61152879B007710718F30221D2EBCC6E9BEEAB4 EA77A872DB2BBA37A9798189CB8A9F0B71B2755 1F119F56390752C6D44874AF982827576FB2733C6 C30329BA3C6BAA0D0951E831F334E2605E5B6687 5038406B581C090FDE4FB95A20D1DAC1A7F80CD 8EB8E013B6C1E178F933F16C3448D653E54ECF' USD+FED688E43D7EEDA8FCCA04564B81B04BB 041FEEA6CE64D711F6D4061A7806F0C6C8D55CF 39624D71FC6A6D6A91073BB25D38E878E9B10F92 BDF7971580368EFBAC28091EC25D09BEF2A04FF 5E363163D5035A9E1A66B2631924DCF24BC5D9E1 86068501E964327030341E061EBEDC878B3C82741 7C4DEDE958034DFBB0C15C1BCD5D5382ACD998 922E9EEA60F8B55E6EE8F55DA5429164783BA6B EC7E2FD09AC1ED9ACA9D303958C2FA522F4C77 8CAA2068E3E64335DC9C41A86C47E3D9A478DC 076057C10EEAD80CE6C0309C8C1BA740A3680F1 0373F1047A1517DF1C9F8862B9D60C099B12EDC2 02FED4593979E56C41A122BEBBD6FE938E02E538 3EAB8BAC' USD+98862F5F151638D2CF2BBB8490F91468C0B5 B20445786741077F3B1525101F0189B3D47C3073A B4D3909944BD8B443934AFF330C434CA46DD586 2615F2CA585080DAF0F5607999BF1549E436CCF3 85A8E5E588B8FF64EC71'	Segmenty USD obsahují filtrovanou šifrovanou původní zprávu.
UNT+9+236'	Patička zprávy, zpráva obsahuje 9 segmentů (včetně služebních).
UNZ+1+000010033'	Patička souboru výměny, soubor výměny obsahuje 1 zprávu.

Správa klíčů

Obecné zásady

Pro implementaci bezpečnostních funkcí pro EDI systém byly zvoleny kryptografické algoritmy, které vyžadují pro svoji funkci parametry - tzv. klíče. Tyto klíče se dělí do několika typů. Dále jsou definovány pravidla tvorby, distribuce, uložení, rušení a práce s klíči podle jejich typu a použití - tzv. pravidla správy klíčů. Tyto pravidla tvoří nedílnou součást implementace systému a musí být proto dodržena všemi subjekty v systému, neboť tvoří základní podmínku správné funkce implementovaných bezpečnostních funkcí.

Klíče, které jsou využívány v systému, jsou následující:

Tajný klíč - tajný klíč je používán jako parametr pro RSA algoritmus, klíč se používá pro vytvoření digitálního podpisu zprávy (nebo certifikátu v případě CA) a k dešifrování DES klíče v došlé zprávě CIPHER. Tajný klíč je přístupný pouze jednomu subjektu - svému vlastníku. Při uložení a používání tajného klíče musí být implementovány dodatečné funkce řízení přístupu ke klíči tak, aby nebyl dostupný v otevřené podobě.

Veřejný klíč - veřejný klíč je používán jako parametr pro RSA algoritmus, klíč se používá pro ověření digitálního podpisu zprávy a pro šifrování DES klíče při utajení odesílaných zpráv. Veřejný klíč se skládá ze dvou částí: exponentu a modulu, které jsou prezentovány jako celá čísla. Veřejný klíč se běžně vyskytuje v systému ve formě **certifikátu.** Certifikáty mohou být distribuovány mezi všechny subjekty v systému.

Pár klíčů - veřejný a tajný klíč, které byly vygenerovány společně a jsou tedy komplementární (text šifrovaný veřejným klíče lze dešifrovat klíčem veřejným a naopak).

Symetrický (DES) klíč - tento klíč je používán jako parametr pro DES algoritmus (ostatní parametry jsou definovány pevně). DES klíč je používán pro šifrování textu zprávy. DES klíč je generován náhodně pro každou šifrovanou zprávu a je následně šifrován RSA algoritmem a přenášen zprávou CIPHER.

Otevřená podoba klíče - je uložení klíče, kdy je klíč v uložen v té podobě, v jaké vstupuje do šifrovacího algoritmu. Tajný klíč se nesmí vyskytovat v otevřené podobě, kromě využití v zabezpečovacím systému.

Zabezpečovací systém - je souhrn software a hardware, na kterém probíhají šifrovací funkce potřebné pro zabezpečení zpráv, které používají klíče.

Další odstavce popisují především správu klíčů pro tajný a veřejný RSA klíč, správě DES klíčů je věnován odstavec Pravidla pro práci se symetrickými klíči.

Povinnosti subjektu

Subjekt je povinen seznámit se s pravidly správy klíčů a tato pravidla dále dodržovat. Pravidla správy klíčů se stávají pro subjekt závazná v okamžiku registrace subjektu u CA.

V případě, že subjekt nebude dodržovat pravidla správy klíčů, bude mu zrušena jeho registrace u CA, budou zrušeny všechny jeho certifikáty, tím pádem subjekt nebude moci dále využívat bezpečnostních funkcí systému.

Generování klíčů

Každý subjekt musí mít program pro vygenerování páru klíčů, který musí splňovat následující vlastnosti:

- Generování klíčů nemůže být přímou součástí programu pro zabezpečování zpráv, program musí být samostatný (nicméně je součástí zabezpečovacího systému).
- Základem pro generování klíčů musí být náhodné (nebo pseudonáhodné) číslo, aby bylo zaručeno, že nebude vygenerován stejný pár klíčů pro různá spuštění programu. Za žádných okolností nesmí být možné spustit program tak, aby generoval stejné páry klíčů.
- Vygenerované klíče musí splňovat požadavky na tzv. silné RSA klíče podle Gordonových kritérií (viz Literatura 17).
- Při hledání prvočísel pomocí pravděpodobnostních testů musí být pravděpodobnost chyby menší než 2^{-30}.
- Program musí umožňovat vygenerování páru klíčů o dané velikosti (tedy 1024 bitů), kdy modulus musí mít nenulový první bit pro danou maximální velikost (tj. pro maximální velikost 1024 bitů musí být modulus v rozsahu $< 2^{1023}, 2^{1024} -1>$).
- Program musí umožnit přiřadit páru klíčů identifikaci, která je uložena s klíči a umožňuje identifikovat oba klíče páru. Identifikace klíče musí být unikátní pro každý generovaný pár. Pro veřejný klíč je tato identifikace uvedena v certifikátu v prvku S500:0538 (Jméno klíče).
- Vygenerovaný tajný klíč je uložen způsobem, který zajistí kontrolu přístupu ke klíči (viz odstavec Pravidla pro lokální uložení klíčů a certifikátů). Není možné aby výstupem z generátoru klíčů byl tajný klíč v otevřené podobě nebo aby tajný klíč byl v rámci programu otevřeně přístupný.
- Vygenerovaný veřejný klíč je uložen v otevřené formě, je vhodné jej již ukládat v takové podobě, která může být přímo předána CA (viz odstavec Certifikace klíčů).

Generování klíčů provádí subjekt pro následující účely:

- Vygenerování iniciačního páru klíčů pro danou bezpečnostní funkci (podpis, šifrování)
- Vygenerování páru klíčů, který nahradí stávající pár klíčů pro určitou funkci (stávající pár klíčů má zrušenou platnost nebo mu platnost brzy vyprší).
- Vygenerování páru klíčů pro rozšíření určité bezpečnostní funkce (např. využití dvou podpisů, nebo různých podpisů pro různé partnery).

Je nutné omezit počet generovaných párů na páry, které jsou potřebné pro zajištění požadovaných bezpečnostních funkcí, je nevhodné provádět generování klíčů, které potom nebudou pro bezpečnostní funkce využity. Pro všechny vygenerované páry klíčů veřejný klíč musí být vždy certifikován, před tím než se začne pár využívat.

Při generování je nutné vytvořit záložní kopie klíčů, které potom subjekt uloží bezpečným způsobem (viz. odstavec Pravidla pro lokální uložení klíčů a certifikátů).

Certifikace klíčů

Před prvním použitím páru klíčů musí být veřejný klíč certifikován.
Pro certifikaci plní CA dvě funkce:

Registrace subjektů - CA registruje subjekty, které využívají její služby, jednoznačně ověří jejich identitu a přidělí jim unikátní identifikaci. Registrace musí předcházet samotné certifikaci klíčů.

Certifikace klíčů - CA certifikuje klíče tj. ověří autenticitu klíče a vytvoří certifikát, kde je veřejný klíč svázán s identifikací subjektu, certifikát je opatřen podpisem CA.

Postup při registraci subjektů:

- Subjekt vyplní registrační formulář, kde uvede:
  - Jméno a adresu subjektu
  - Jména a kontakty osob určených subjektem pro styk s CA
  - Vzorové podpisy kontaktních osob
  - Určení způsobu předávání dat mezi subjektem a CA (pošta, on-line, osobně)
  - Prohlášení o dodržování stanovené politiky správy klíčů,
  - Datum
  - Podpis odpovědného zástupce subjektu a razítko
- Subjekt předá registrační formulář CA
- Subjekt musí prezentovat schopnost dodržet požadovaná pravidla správy klíčů, eventuálně uvést způsob implementace bezpečnostních funkcí.
- CA zaregistruje subjekt a přidělí mu jednoznačné EDI ID, které nadále bude subjekt uvádět ve všech identifikacích svých klíčů (EDIFACT prvek S500:511). EDI ID je uvedeno do registračního formuláře, jehož kopii subjekt obdrží.

Postup při certifikaci klíčů je následující:

- Před certifikací musí být subjekt registrován.
- Určený pracovník předá CA veřejný klíč a certifikační formulář, předání je možné osobně, nebo pomocí doporučené pošty. Certifikační formulář je nutné předat CA v každém případě, neboť představuje formální vyjádření odpovědnosti strany za vygenerované digitální podpisy a jednoznačně váže danou stranu ke jejímu klíči.

Pro předání veřejného klíče existuje několik možností:

- Veřejný klíč určený pro certifikaci je uložen v textovém souboru, tento vyhovuje syntaktickým pravidlům UN/EDIFACT a obsahuje segmenty USC a USA (tedy vlastně certifikát bez segmentu USR s podpisem certifikátu). Soubor je uložen na dohodnutém magnetickém médiu.
  Přesná syntaxe segmentů certifikátu je uvedena v kapitole Implementace digitálního podpisu (skupina segmentů 2). V segmentech musí být vyplněny prvky dle následující tabulky:

Segment	Prvek	Opakování	Hodnota

USC	S500:577	1:1	‘3’
USC	S500:538	1:1	Identifikace páru klíčů
USC	S500:511	1:1	Přidělené EDI ID subjektu
USC	S500:586	1:1-3	Pokud jsou prvky uvedeny, jsou převzaty do certifikátu
USC	505	1	'2' kód použitého filtru (viz kapitola Implementace digitálního podpisu)
USA	S502:0523	1:1	'6' nebo '7' (podle využití klíče, viz kapitola Implementace digitálního podpisu)
USA	S502:525	1:1	'0'
USA	S502:527	1:1	'10'
USA	S503:532	1:1	Délka modulu dekadicky
USA	S503:531	1:1	‘14’
USA	S503:532	2:1	Exponent veřejného klíče, filtrovaný
USA	S503:531	2:1	‘13’
USA	S503:532	3:1	Modulus veřejného klíče, filtrovaný
USA	S503:531	3:1	‘12’

Pozn. Počet opakování je vyjádřen jako (opakování prvku, složeného prvku) : (opakování prvku ve složeném prvku - pouze pro složené prvky).

Magnetické médium, na kterém je soubor s veřejným klíčem, je předáváno jako příloha k certifikačnímu formuláři a musí být označeno následovně:
- nápisem - "Veřejný klíč :" Identifikace klíče (stejná jako uvedena v S500:538)
- nápisem - "Organizace:" EDI ID subjektu
- nápisem - "Datum:" datum vygenerování klíčů

  - Veřejný klíč může být uveden přímo v certifikačním formuláři, kdy modulus a exponent veřejného klíče jsou hexadecimálním tvaru (platí stejná pravidla jako filtrování binárních dat hexadecimálním filtrem, viz kapitola Implementace digitálního podpisu). Tento způsob není však doporučen pro velké riziko chyby ve veřejném klíči.
- Certifikační formulář obsahuje:
  - Jméno a adresu subjektu
  - EDI ID subjektu
  - Algoritmus, ke kterému se váží klíče (tedy RSA)
  - Velikost klíče (tedy 1024 bitů)
  - Identifikace klíče (stejná jako uvedena v EDIFACT USC S500:538)
  - Datum vygenerování klíčů
  - Požadovaný počátek platnosti certifikátu
  - Použití tajného klíče (podpis, šifrování symetrického klíče, obojí)
  - Nepovinně identifikaci vlastníka certifikátu (stejná jako uvedena v S500:586), kdy se jedná o bližší určení subjektu, jeho pobočky a vlastníka certifikátu nebo funkce klíče.
  - Nepovinně hexadecimální zápis veřejného klíče (pokud není doručen CA jiným způsobem).
  - Datum
  - Podpis kontaktní osoby (uvedené v registračním formuláři)
- Po převzetí certifikačního formuláře a veřejného klíče ověří CA uvedené údaje, případně může kontaktovat subjekt pro ověření určitých údajů. Po ověření všech údajů provede CA

certifikaci klíče a vytvoří certifikát, který opatří digitálním podpisem pomocí svého tajného klíče. Pro podpis certifikátu jsou použity algoritmy MD5 a RSA.
Pár klíčů, který používá CA pro digitální podpis certifikátu, je využíván pouze pro tento účel, pokud CA komunikuje s uživateli on-line pomocí zprávy KEYMAN, používá pro tento účel jiný pár klíčů, kdy je veřejný klíč z páru certifikován běžným způsobem.
Certifikát je uložen v databázi CA.
Certifikát obsahuje údaje dodané subjektem, přičemž ale CA nemusí dodržet požadovaný počátek platnosti. CA doplní certifikát o další údaje, především o platnost certifikátu, referenční číslo certifikátu, identifikaci CA a klíče CA.
Maximální doba, která uplyne mezi převzetím certifikačního formuláře a veřejného klíče a certifikací veřejného klíče je 7 dní.
V případě, že nelze certifikaci provést vyrozumí CA subjekt doporučeným dopisem a eventuálně telefonicky nebo e-mailem do výše uvedeného termínu.

- Certifikát je následně předán subjektu, kdy je zvolen způsob předání specifikovaný v registračním formuláři. Spolu s certifikátem je předán i certifikační protokol, který obsahuje:
  - Jméno a adresu CA
  - EDI ID CA
  - Jméno a adresu subjektu
  - EDI ID subjektu
  - Referenční číslo certifikátu (prvek 0536)
  - Identifikace klíče (stejná jako uvedena v S500:538), který byl použit pro podpis certifikátu
  - Datum vygenerování certifikátu
  - Platnost certifikátu od - do
  - Datum
  - Podpis zástupce CA
- Certifikát je uložen do textového souboru. Soubor je uložen na dohodnutém magnetickém médiu, které je označeno:
  - nápisem - "Certifikát:" - Referenční číslo certifikátu (prvek 0536)
  - nápisem - "Veřejný klíč :" - Identifikace klíče subjektu (prvek S500:538)
  - nápisem - "Organizace:" - EDI ID subjektu
  - nápisem - "Datum:" - Datum vygenerování certifikátu

Způsoby pro předání certifikátu jsou:

- Kontaktní osoba si certifikát spolu s certifikačním protokolem vyzvedne osobně u CA.
- Certifikát je uložen do souboru dle předcházejícího odstavce a je spolu s certifikačním protokolem zaslán jako doporučená zásilka na adresu subjektu.

Platnost klíčů

Platnost páru klíčů je daná platností certifikátu veřejného klíče. Postup pro ověření platnosti certifikátu je následující:

1. Je ověřena syntaktická správnost certifikátu (podrobná syntaxe certifikátu viz kapitola Implementace digitálního podpisu).
2. Je ověřena časová platnost - aktuální datum a čas musí být v rozmezí platnost od, platnost do (prvek S501) specifikovaném v certifikátu.
3. Je ověřen status certifikátu (prvek 0567). Certifikát musí být platný, tj. prvek 0567 = 1, nebo prvek není uveden.
4. Certifikát je ověřen proti seznamu zrušených certifikátů, nesmí se v něm vyskytovat (identifikace dle referenčního čísla). Seznam zrušených certifikátů je vydáván CA, implementace u subjektu jej má lokálně uložen (viz odstavec Rušení certifikátů a Pravidla pro lokální uložení klíčů a certifikátů).
5. Je ověřen digitální podpis certifikátu (podrobnosti o algoritmu podpisu certifikátu viz kapitola Implementace digitálního podpisu). Pro ověření podpisu certifikátu je nutné mít veřejný klíč CA z páru, který byl použit pro podpis certifikátu. Potřebný klíč je identifikován v prvku S500:538. Tento klíč je distribuován mezi subjekty opět ve formě certifikátu CA(viz odstavec Distribuce certifikátů). Certifikát veřejného klíče CA nesmí být zrušen (může však mít prošlou platnost), jinak je nutné považovat ověřovaný certifikát za neplatný.

Veřejný klíč může být používán pro ověření digitálního podpisu nebo zašifrování symetrického klíče pouze tehdy, pokud byl ověřen příslušný certifikát, který veřejný klíč obsahuje, a byly splněny výše uvedené kontroly. Výjimku tvoří případ, kdy jsou certifikáty uchovávány v lokální databázi zabezpečovacího systému a byly při uložení kompletně ověřeny (viz odstavec Pravidla pro lokální uložení klíčů a certifikátů). V tomto případě je možné používat veřejné klíče bez kontroly certifikátu, nicméně při každém použití veřejného klíče je nutné ověřit jeho časovou platnost podle údajů uvedených v certifikátu (bod 2. kontroly).

Veřejný klíč nesmí být používán pro zašifrování symetrického klíče, pokud je certifikát veřejného klíče neplatný nebo pokud byl certifikát zrušen (počítá se okamžik, kdy subjekt získá a zpracuje informaci o zrušení certifikátu - viz odstavec Rušení certifikátů).

Podpis ověřený pomocí veřejného klíče, jehož certifikát je neplatný nebo byl zrušen, nesmí být při výměně zpráv pokládán za platný. Výjimku tvoří ověřování archivovaných zpráv, kdy ale musí být při zpracování zprávy v systému subjektu rozlišeno, že se jedná o archivovanou zprávu.

Tajný klíč může být používán pro digitální podpis zprávy nebo dešifrování symetrického klíče pouze tehdy pokud subjekt má certifikát veřejného klíče z odpovídajícího páru, certifikát je zaveden v zabezpečovacím systému a tento certifikát je platný a nebyl zrušen. V případě, že se tento certifikát nachází v lokální databázi a byl při uložení kompletně ověřen (viz odstavec Pravidla pro lokální uložení klíčů a certifikátů), není nutné při použití tajné klíče ověřovat celý certifikát, stačí ověřit pouze časovou platnost certifikátu (bod 2.).

Výjimkou je pouze dešifrování symetrického klíče v archivovaných zprávách, kdy lze použít neplatné tajné klíče, ale musí být při zpracování zprávy v systému subjektu rozlišeno, že se jedná o archivovanou zprávu.

Standardní doba platnosti certifikátu je 1 rok.

Před vypršením platnosti certifikátu (ne však dříve než 21 dnů před) je subjekt povinen vygenerovat dvojici klíčů, která nahradí stávající dvojici pro danou bezpečnostní funkci, a provést certifikaci veřejného klíče a další činnosti tak, aby nový pár mohl být používán před ukončením platnosti páru starého.

Začátek platnosti certifikátu veřejného klíče z nového páru klíčů musí být 7-21 dní před ukončením platnosti certifikátu veřejného klíče ze starého páru klíčů, tak aby byla umožněna průběžná výměna klíče.

.

Distribuce certifikátů

Certifikační autorita distribuuje certifikáty mezi subjekty, certifikáty jsou předávány subjektům ve formě textového souboru. Soubor obsahuje certifikáty v UN/EDIFACT tvaru, soubor může obsahovat více certifikátů, kdy další certifikát bezprostředně následuje za znakem ukončení segmentu certifikátu předchozího. Soubor je uložen na dohodnutém magnetickém médiu, které je označeno:

- nápisem - "Certifikáty:" - Bližší specifikace certifikátů v souboru
- nápisem - "CA:" ID - Certifikační autority
- nápisem - "Datum:" - Datum vytvoření souboru

A) Iniciační distribuce certifikátů

Při registraci subjekt obdrží certifikát CA, který obsahuje veřejný klíč CA používaný pro podpisy certifikátů. Jedná se o standardní UN/EDIFACT certifikát, tento certifikát je podepsán tajným klíčem z páru, ke kterému patří veřejný klíč obsažený v certifikátu, může být tedy ověřen bez další znalosti.

Certifikát CA musí zástupce subjektu vyzvednout osobně a je mu předán ve formě souboru (viz výše).

Dále může zástupce subjektu při registraci také obdržet existující certifikáty potřebné pro další komunikaci, požadované certifikáty může identifikovat pomocí čísel certifikátů (EDIFACT prvek 0536), EDI ID vlastníka certifikátu (EDIFACT prvek S500:0511) a identifikace klíče (EDIFACT prvek S500:0538).

B) Distribuce certifikátů na požadavek

Dále kdykoliv po registraci může subjekt kontaktovat CA a vyžádat si certifikáty, které potřebuje pro svou komunikaci, požadované certifikáty může identifikovat pomocí čísel certifikátů (EDIFACT prvek 0536), EDI ID vlastníka certifikátu (EDIFACT prvek S500:0511) a identifikace klíče (EDIFACT prvek S500:0538). Požadavek na určité certifikáty je možné předávat písemně: buď poštou, faxem nebo e-mailem.

Certifikáty mu budou zaslány na magnetickém médiu v souboru ve standardním tvaru (viz výše) pomocí doporučené pošty, nebo si soubor může vyzvednou zástupce subjektu osobně u CA.

C) Pravidelná distribuce certifikátů

Kromě výše uvedených případů distribuuje CA certifikáty mezi uživatele přímo, bez nutnosti předchozího vyžádání certifikátů. Jedná se o tyto případy:

- Distribuce seznamu zrušených certifikátů. Tento seznam je distribuován mezi uživatele vždy při změně tohoto seznamu (podrobněji viz odstavec Rušení certifikátů).
- Distribuce nových certifikátů. CA může distribuovat nové certifikáty určitých subjektů, po dohodě s těmito subjekty, mezi všechny subjekty systému.

Certifikáty jsou subjektům zasílány na magnetickém médiu v souboru ve standardním tvaru (viz výše) pomocí doporučené pošty, nebo si soubor může vyzvednou zástupce subjektu osobně u CA.

Speciální případ tvoří distribuce nového certifikátu CA. Jedná se o certifikát veřejného klíče z páru, který bude využíván pro podpis certifikátů a nahradí stávající pár. CA vyrozumí subjekty o výměně svých klíčů minimálně 14 dní před začátkem platnosti nové páru, pomocí doporučeného dopisu. Zástupce subjektu musí vyzvednout nový certifikát CA osobně u CA, kdy certifikát je předán ve formě souboru na dohodnutém magnetickém médiu (stejně jako v odstavci A).

Rušení certifikátů

CA může zrušit platnost určeného certifikátu, což znamená zrušení platnosti páru klíčů.

Zrušení platnosti certifikátu může proběhnout z následujících důvodů:

- Prozrazení tajného klíče vlastněného subjektem
- Odůvodněné podezření na prozrazení tajného klíče vlastněného subjektem
- Ztráta nebo zničení tajného klíče vlastněného subjektem (včetně záložních kopií)
- Prozrazení tajného klíče CA (v tomto případě je zrušen certifikát CA)
- Změna údajů uvedených v certifikátu
- Ukončení platnosti certifikátu, protože daný pár klíčů nebude dále využíván.

Subjekt žádá o zrušení certifikátu pomocí žádosti o zrušení certifikátu, která může být zaslána na adresu CA pomocí doporučené pošty nebo faxem. V nezbytném případě je možné vyžádat zrušení certifikátu telefonicky, kdy je nutné uvést všechny údaje obsažené v žádosti o zrušení certifikátu a žádost o zrušení certifikátu je odeslána následně. CA může ověřit oprávněnost a správnost žádosti o zrušení certifikátu telefonickým dotazem u subjektu.

Žádost o zrušení certifikátu musí obsahovat:

- Jméno a adresu subjektu
- EDI ID subjektu
- Číslo certifikátu (stejné jako je uvedeno v EDIFACT prvku 0536)
- Identifikace klíče (stejná jako uvedena v EDIFACT prvku S500:538)
- Důvod pro zrušení certifikátu
- Datum
- Podpis kontaktní osoby (uvedené v registračním formuláři)

Subjekty jsou informovány o zrušení certifikátu ve formě seznamu zrušených certifikátů (CRL - Certificate Revocation List), který obsahuje všechny certifikáty, které jsou zrušeny (tj. CA změnila jejich status v EDIFACT prvku 0567) a přitom platí z časového hlediska (tj. pro platnost uvedenou v certifikátu v prvcích S501).

Seznam je uložen v souboru, kde jsou uloženy kompletní certifikáty stejným způsobem, jak je popsáno v odstavci Distribuce certifikátů. Způsob distribuce je opět popsán v odstavci Distribuce certifikátů.

CA generuje tento seznam a distribuuje jej mezi subjekty při změně seznamu, tedy pokud je zrušen certifikát a přidán do seznamu.

V případě nutnosti může CA vyrozumět subjekty o zrušení určitého certifikátu telefonicky, faxem nebo e-mailem.

Subjekt, který si vyžádal zrušení certifikátu, obdrží od CA protokol o zrušení certifikátu, který obsahuje:

- Jméno a adresu CA
- EDI ID CA
- Jméno a adresu subjektu
- EDI ID subjektu
- Číslo certifikátu (stejné jako je uvedeno v EDIFACT prvku 0536)
- Identifikace klíče (stejná jako uvedena v EDIFACT prvku S500:538)
- Důvod pro zrušení certifikátu
- Datum zrušení certifikátu.
- Datum
- Podpis zástupce CA

Protokol o zrušení certifikátu je subjektu zaslán doporučenou poštou.

Ve výjimečných případech, kdy je výrazně ohrožena bezpečnost systému, může CA zrušit certifikát subjektu bez předchozí žádosti subjektu. Subjekt je potom vyrozuměn o zrušení certifikátu zasláním protokolu o zrušení certifikátu a seznamu zrušených certifikátů.

Souhrnně lze definovat postup pro zrušení certifikátu následně:

1) Subjekt zašle žádost o zrušení certifikátu CA.
2) CA ověří oprávněnost a správnost žádosti a zruší certifikát. Zrušení certifikátu proběhne tak, že CA změní v EDIFACT certifikátu hodnotu prvku 0567 (Bezpečnostní status) na:
   - hodnotu "2" - certifikát zrušen, v případě že se jedná o bezpečnostní důvody, tj. byl ohrožen tajný klíč subjektu
   - hodnotu "4" - certifikát byl ukončen z formálních důvodů
3) Dále je v certifikátu vyznačeno datum a čas zrušení certifikátu (místo datumu a času vygenerování certifikátu).
4) Certifikát je potom opět podepsán tajným klíčem CA.

5) Zrušený certifikát je zařazen do seznamu zrušených certifikátů, který je potom distribuován mezi subjekty.
6) Maximální doba od přijetí žádosti na zrušení certifikátu do zrušení certifikátu a distribuce seznamu zrušených certifikátů je 4 pracovní hodiny (jedná se o běžné hodiny pracovní doby, pokud bude žádost o zrušení certifikátu přijata po 16 hodině, budou seznamy zrušených certifikátů distribuovány až další den).
7) CA zašle protokol o zrušení certifikátu subjektu, který žádal o zrušení certifikátu.
8) Subjekty (včetně subjektu, který žádal zrušení certifikátu) obdrží seznam zrušených certifikátů, tyto seznamy musí co nejdříve zavést do svého zabezpečovacího systému.

Pravidla pro lokální uložení klíčů a certifikátů

Pro uložení klíčů u subjektu platí následující pravidla:

A) Pravidla pro uložení tajných klíčů

- Tajný klíč musí vždy uložen tak (s výjimkou uložení klíče v zabezpečovacím systému), aby byla zajištěno řízení přístupu ke klíči na úrovni přístupového hesla o minimální délce 8 znaků. Bez znalosti tohoto hesla nesmí být možné získat otevřenou podobu klíče, ani ho používat pro digitální podpis či dešifrování zprávy. Vhodným mechanismem pro ochranu tajného klíče je např. jeho zašifrování pomocí klíče odvozeného z přístupového hesla, či jeho uložení na Smart Card.
- Zabezpečení tajného klíče se musí provést již během jeho vygenerování v rámci jednoho programu (generátoru klíčů). Je nepřípustné, aby výstupem z generátoru klíčů byl tajný klíč v otevřené podobě a jeho zabezpečení se provedlo následně.
- Při generování klíčů musí být vytvořeny 3 kopie tajného klíče. Jedna kopie bude využívána jako aktuální klíč, druhé dvě kopie budou uloženy jako záložní kopie. Každá kopie, pokud je uložena na magnetickém médiu, kartě atd., musí být označena EDI ID organizace a identifikací klíče.

Pro zabezpečení záložních kopií tajného klíče platí stejná pravidla jako pro aktuální tajný klíč.

Záložní kopie musí být uloženy tak, aby byla zajištěna jejich fyzická bezpečnost a bylo možné omezit přístup k těmto kopiím. Záložní kopie musí být uloženy odděleně od aktuálního klíče. Vhodným prostředkem pro uložení záložních kopií je např. trezor.

Vlastník klíče by měl mít přístup k těmto kopiím.

- Přístupové heslo k tajnému klíči může znát pouze jedna osoba tzv. vlastník klíče, který toto heslo zadá při iniciačním zabezpečení klíče. (ve speciálních případech je možné, aby heslo znalo i více osob, jejich okruh však musí být omezen). Vlastník klíče může přístupové heslo ke klíči změnit.

Vlastník klíče musí být seznámen s pravidly správy klíčů.

Vlastník klíče také vlastní klíč fyzicky (pokud je uložen na magnetickém médiu, Smart Card aj.) a odpovídá za jeho odpovídající použití v souladu s pravidly správy klíčů.

- Přístupové heslo se nesmí vyskytovat nikde v otevřené podobě, s výjimkou jeho zadání při zabezpečení klíče, při zavedení klíče do zabezpečovacího systému (v těchto případech se však přístupové heslo nesmí čitelně zobrazit) a může být uloženo spolu se záložními kopiemi klíče, kdy ale musí být zajištěna jeho dodatečná ochrana před jeho prozrazením, např. uložením v zapečetěné obálce.
- Tajný klíč se může vyskytovat v otevřené podobě pouze v zabezpečovacím systému. K takto uloženému klíči musí být řízen přístup systémovými prostředky. V případě, že klíč nebude zabezpečovacím systémem dále využíván, musí systém umožnit vymazání klíče tak, aby následně nebylo možné získat jeho otevřenou podobu žádnými systémovými prostředky.

V případě, že je i zabezpečený tajný klíč trvale uchováván v zabezpečovacím systému, je nutné zajistit navíc řízení přístupu k tomuto klíči systémovými prostředky.

- V případě, že dojde k poškození nebo ztrátě aktuálního tajného klíče, je možné použít záložní kopii klíče, kdy jedna ze záložních kopií může být použita jako aktuální klíč a musí být doplněn počet záložních kopii.
- Subjekt je povinen archivovat tajné klíče, kterým vypršela doba platnosti. Pro tento klíč musí existovat alespoň dvě archivní kopie. Pro archivní kopie platí stejná pravidla jako pro záložní kopie (nelze je však použít jako aktivní klíč) a musí být uloženy obdobným způsobem, nesmí však dojít k jejich záměně.
- Archivní kopie tajných klíčů musí být uchovávány minimálně po dobu 10 let od data ukončení platnosti klíče (viz odstavec Platnost klíčů).
- Subjekt je povinen okamžitě informovat CA o jakémkoli pokusu o zneužití tajného klíče, o získání klíče v otevřené podobě, či ztrátě tajného klíče.

B) Uložení certifikátů a veřejných klíčů:

- Veřejný klíč se v otevřené podobě mimo certifikát může vyskytovat pouze po vygenerování páru (kdy je poslán na CA) a v zabezpečovacím systému po dobu nutnou pro jeho použití v šifrovací funkci. Jinak veřejný klíč musí být uložen ve formě certifikátu podepsaného CA.
- Po vygenerování páru klíčů musí subjekt vytvořit alespoň jednu záložní kopii veřejného klíče, která musí být uložena tak, aby byla zajištěna její fyzická bezpečnost, do doby kdy subjekt obdrží a ověří certifikát svého veřejného klíče.
- V zabezpečovacím systému musí být uloženy certifikáty subjektu (nebo uloženy tak, aby byly zabezpečovacímu systému dostupné při zabezpečení/kontrole zabezpečení zpráv) a dále tam mohou být uloženy další certifikáty, které jsou využívány pro komunikaci .
- Veřejné klíče z certifikátů, které jsou uloženy v zabezpečovacím systému, lze používat i bez úplného ověření certifikátu (viz odstavec Platnost klíčů), pokud jsou splněny následující podmínky:
- Certifikát je časově platný (a je označen jako platný.
- Certifikát byl při uložení v zabezpečovacím systému plně zkontrolován a v případě, že byl neplatný, nebyl uložen, nebo byl označen jako neplatný.

- Při příjmu (uložení) seznamu zrušených certifikátů jsou všechny certifikáty uložené v zabezpečovacím systému zkontrolovány proti seznamu, ty které se na seznamu vyskytují jsou označeny jako neplatné.
- Všechny certifikáty uložené v zabezpečovacím systému jsou zkontrolovány při změně klíče CA.
- Existuje funkce, která umožňuje kdykoliv kompletně zkontrolovat certifikáty uložené v zabezpečovacím systému.
- Veřejný klíč CA je uložen na zabezpečovacím zařízení ve formě certifikátu CA.
  Při uložení certifikátu CA, subjekt musí mít absolutní jistotu, že se opravdu jedná o soubor s platným certifikátem CA, neboť tento tvoří základ zabezpečení sytému. Je vhodné autenticitu certifikátu CA zajistit nějakým dodatečným způsobem, např. zpětné ověření u CA pomocí telefonátu aj. Při uložení certifikátu CA musí být zkontrolován jeho podpis. V dalším provozu je vhodné, aby certifikát CA byl uložen na zabezpečovacím zařízení tak, aby byla zajištěna jeho integrita a kontrola přístupu k certifikátu CA po dobu používání (speciálními službami nebo využitím systémových služeb).
- Na zabezpečovacím zařízení musí být uložen poslední (nejaktuálnější) seznam zrušených certifikátů distribuovaný CA. Při uložení seznamu zrušených certifikátů musí být proběhnout kontrola podpisu certifikátů. Tento seznam je používán pro kontrolu platnosti certifikátů.

C) Uchování dokumentů spojených s klíči

- Subjekt je povinen uchovávat kopii registračního formuláře po celou dobu využití bezpečnostních funkcí systému (jinými slovy pokud využívá tajné a veřejné klíče).
- Subjekt je povinen uchovávat následující dokumenty po stejnou dobu, po kterou uchovává kopii tajného klíče z páru, který je uveden v dokumentech (viz odstavec A):
- kopii certifikačního formuláře
- certifikační protokol
- kopii žádosti o zrušení certifikátu
- protokol o zrušení certifikátu
- Dokumenty musí být uchovávány tak, aby bylo zabráněno jejich zničení a zneužití.

Pravidla pro práci se symetrickými klíči

Symetrické klíče se používají pro algoritmus DES pro šifrování/dešifrování zprávy. Platí pro ně následující pravidla:

- Symetrický klíč se v otevřené podobě smí vyskytovat pouze v zabezpečovacím systému.
- Symetrický klíč se generuje náhodně (pseudonáhodně) pro účel zašifrování jedné zprávy. Tento klíč nesmí být dále použit pro šifrování dalších zpráv, pro každou další zprávu musí být klíč generován znovu.

- Po využití symetrického klíče (pro šifrování/dešifrování zprávy) musí být symetrický klíč v otevřené podobě vymazán, tak aby následně nebylo možné získat jeho otevřenou podobu žádnými systémovými prostředky.

Parametry použitých kryptografických algoritmů

RSA (Rivest, Shamir, Adleman)
Parametry:
- délka modulu: 1024 bitů
- exponent veřejného klíče: pevně volený 10001H (65537) - čtvrté Fermatovo číslo (F4)
- specifikace dle použité literatury bod 7)

MD5 (Message Digest Algorithm 5)
Parametry:
- specifikace dle použité literatury bod 12)

DES (Digital Encryption Standard)
Parametry:
- operační mód CBC (Cipher Block Chaining)
- hodnota IV (Inicialisation Value) = '00 00 00 00 00 00 00 00' H
- doplňovací znak (Padding Character) = 00H
- specifikace dle použité literatury bod 11)

Pozn.: V počátečním období se připouští použití libovolných realizací výše zmíněných algoritmů, v dalším vývoji je nutno počítat zejména s následujícími trendy:

- rozšiřování počtu druhů o modernější algoritmy

- regulaci variety přípustných řešení algoritmů v souladu s globální bezpečnostní politikou. Důraz bude kladen především na soulad s mezinárodními standardy a na certifikaci produktů.

Závěr

Výše popsané řešení je plně založeno na mezinárodních standardech, a tak poskytuje široké možnosti pro implementaci. Toto řešení je také otevřené z hlediska implementace v UN/EDIFACT a je používáné i v dalších EDI aplikacích.

Literatura

1) X.200 ITU(CCITT) Recommendation " Open Systems Interconnection", 1988

2) X.400 - 420 ITU(CCITT) Recommendations "Message Handling System", 1988

3) X.435 ITU(CCITT) Recommendation "Electronic Data Interchange Messaging System" (Geneva 1991)

4) X.509 ITU(CCITT) Recommendation "Open Systems Interconnection - The Directory - Authentication Framework", 1991

5) Digital Signatures in EDIFACT; TEDIS Programme 1990

6) Security in Open Enviroment; TEDIS II 1992

7) Rivest R. L., Shamir A., Adleman L. :Method of Obtaining Digital Signatures and Public Key Cryptosystems; Comm. of ACM Feb. 1978

8) UN/TRADE/WP.4/R.1026 "EDIFACT Security Implementation Guidelines", 1994

9) ISO 9735 (ČSN ISO 9735) "UN/EDIFACT Syntax Rules"

10) ISO/DIS 11166 "Key Management by Means of Asymmetric Algorithms", 1991

11) ANSI X3.92-1981 (ISO 8731-1, ISO 8792) Data Encryption Standard (DES)

12) Rivest R.: RFC 1321 - The MD5 Message Digest Algorithm , April 1992

13) ISO/CD 9735 - 5 "Security Rules For Batch EDI", 1995

14) ISO/CD 9735 - 6 " Secure Authentication And Acknowledgement Message (AUTACK)", 1995

15) ISO/WD 9735 - 9 "Security Key And Certificate Management (Message KEYMAN), 1995

16) UN - ECE -EDIFACT - SJWG, "Cipher Text Message (CIPHER) Message Implementation Guidelines", 1995

17) Gordon, J.: "Strong RSA Keys", Electronics Letters, 20, 5, strana 514-516

18) PKCS#1: "RSA Encryption standard", RSA Laboratories, 1993