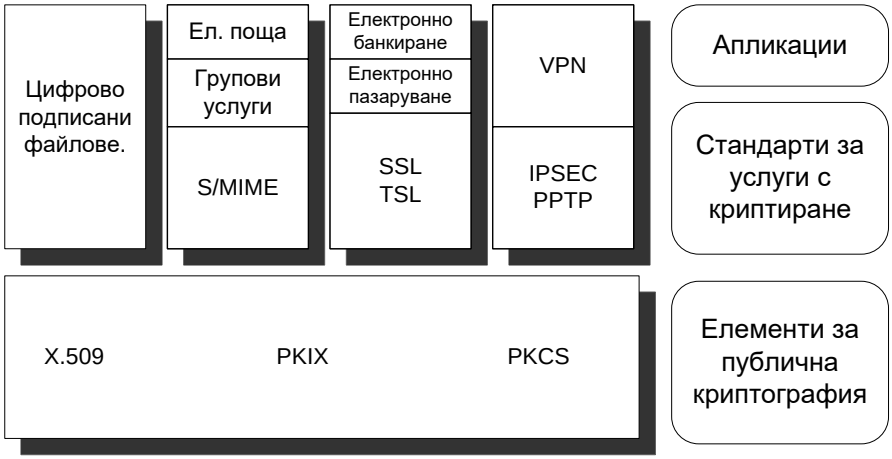
Глава единадесета

СИГУРНОСТ В IP БАЗИРАНИ КОМУНИКАЦИОННИ СИСТЕМИ

11.1 ВЪВЕДЕНИЕ

Защитата на данните за всяко от нивата на OSI модела се реализира по два основни метода:

- криптиране на данните и/или заглавните части на пакетите (header);
- дефинирани от потребителя маршрути;



Фиг. 11.1. Схема на организиране на сигурни комуникационни системи

Както се вижда от Фиг. 11.1, за да се организират сигурни комуникации е необходимо да съществуват различни методи, технически средства и стандарти, чиито комбинации дават възможност да се реализира сигурна услуга.

Сигурни комуникации обхващат четири основни направления:

- защита на файлове, включваща конфиденциалност, интегритет и автентификация;
- защита на електронната поща;
- защита на преноса в транспортния слой (SSL -Secure Socket Layer, TSL -Trusted Socket Layer).
- защита на преноса в мрежовия слой (IPSEC[1] и PPTP[2] добре де – горе се дава пълната дефиниция, а пък тук е с бележка под линия протоколи).

Публичната криптография се разработва на основа на стандартите PKCS – Public Key Cryptography Standards. Създаването на цифрово подписани

[1] Security Internet Protocol

[2] Point to Point Tunelling Protocol.

файлове се основава на стандарт X.509. Използването на сигурна електронна поща или групова услуга изисква наличие на протокол S/MIME[3] .

PKCS стандартите специфицират изискванията за приложение на методите за публична криптография. PKI е спецификация за организиране на инфраструктурата[4] (средата за прилагане) на публичната криптография. В нея се включва и PKIX(public key infrastructure extension) - публична инфраструктура, разработена от работна група на IETF[5]. PKCS[6] обхващат следните стандарти:

- **PKCS #1: RSA CRYPTOGRAPHY STANDARD**
- **PKCS #3: DIFFIE-HELLMAN KEY AGREEMENT STANDARD**
- **PKCS #5: PASSWORD-BASED CRYPTOGRAPHY STANDARD**
- **PKCS #6: EXTENDED-CERTIFICATE SYNTAX STANDARD**
- **PKCS #7: CRYPTOGRAPHIC MESSAGE SYNTAX STANDARD**
- **PKCS #8: PRIVATE-KEY INFORMATION SYNTAX STANDARD**
- **PKCS #9: SELECTED ATTRIBUTE TYPES**
- **PKCS #10: CERTIFICATION REQUEST SYNTAX STANDARD**
- **PKCS #11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD**
- **PKCS #12: PERSONAL INFORMATION EXCHANGE SYNTAX STANDARD**
- **PKCS #13: ELLIPTIC CURVE CRYPTOGRAPHY STANDARD**
- **PKCS #15: CRYPTOGRAPHIC TOKEN INFORMATION FORMAT STANDARD**

Една от предпоставките за развиване на съвременното Internet-общество е възможността за организиране на електронно банкиране и пазаруване. Потребителите ползват обикновено кредитни карти. При покупка електронният магазин изисква от потребителя да въведе номер на кредитна карта, от която да се изтегли финансовата стойност на извършената от потребителя покупка. Номерът на кредитна карта е притежание единствено на нейният потребител и не може да се пренася през Internet-мрежата в открит вид. За целта, преди да бъде формиран съответния пакет за пренасяне, номера на кредитната карта се криптира. От съществено значение е и еднозначното идентифициране на сървъра на магазина. За да се реализират тези две функции са разработени протоколите TSL и SSL.

Друга функция на сигурните комуникации е необходимостта от изграждане на защитени маршрути (тунели) между корпоративните мрежи на двама или повече бизнес- партньори. За да се реализира такъв защитен тунел, се използват протоколите IPSEC и PPTP. На тяхна основа се изграждат **виртуалните частни мрежи (VPN – Virtual Private Networks).**

11.2. ИНФРАСТРУКТУРА НА ПУБЛИЧНИТЕ КЛЮЧОВЕ.

---

[3] Secure ***M**ultipurpose **I**nternet **M**ail **E**xtensions*

[4] Същността на инфраструктурата ще бъде обяснена в края на главата.

[5] Internet Engineering Task Force.

[6] PKCS#2 и PKCS#4 са обединение в PKCS#1.

За да се осигури мениджмънт на криптографията с публични ключове се изгражда инфраструктура, наречена **Public Key Infrastructure (PKI)**. Тя съдържа протоколи, услуги и стандарти, регламентираща употребата на публични криптографски средства. Специфицират се изискванията за изграждане на цялостна сигурна публична система, която гарантира конфиденциалността, интегритета и автентичността на данните, надеждността и сигурността на ресурсите на комуникационните мрежи и автентификацията на страните в един комуникационен процес. Наличието на такава инфраструктура гарантира сигурността на електронната поща, WWW транзакциите, електронната търговия, корпоративните частни мрежи и бизнес приложенията. PKI съдържа мениджмънта на публичните ключове. Мениджмънтът включва:

- процедури по създаване и регистриране на сертификати за публични ключове;
- процедури за унищожаване на сертификати;
- процедури за генериране на публични ключове;
- процедури за оценка на сигурността, валидността и разрешените операции с един сертификат.

За да се осигури дейността по мениджмънта, съществуват две структури – сертифицираща (**Certification Authority)** и регистрираща (**Registration Authority**).

Certification Authority е организация за издаване и удостоверяване на валидността на цифров сертификат Цифровият сертификат представлява електронен документ и се изработва по стандарти ITU-T X.509 и ISO 9594-8, X.509 v3 съгласно ISO. Сертификатът съдържа следните данни:

Таблица 11.1

Version(v3)	Поле съдържащо версията на сертификата
Serial number	Уникално число дадено от легализиращата институция (CA)
Signature algorithm ID	Използван алгоритъм за подписване
Issuer name	X.509 стандарт за името на публикувалата го CA
Validity period	Периода на валидност за сертификата
Subject name	X.509 стандарт за името на сертификата
Subject public key info	Информация за публичния ключ
Issuer unique identifier	Идентификация, удостоверяваща издателя на сертификата
Subject unique identifier	Идентификацията на собственика на сертификата
Extensions	Допълнителна информация[7]

[7] Това поле може да бъде и празно.

Signature	Цифров подпис на CA покриващ всички полета

Документът X.509 свързва на генерирания публичен и секретен ключ към данните за потребителя и организацията, която е издала сертификата. Този документ се публикува в публичен списък (**Certificate-Revocation List CRL)** Публичността е необходима за гарантиране на възможността за справки. Поддържането на такъв списък се налага поради необходимостта от сигнализиране на следните събития: секретният ключ е компрометиран, потребителят на сертификата повече няма права над него, сертификатът е с изтекъл период на валидност и др.

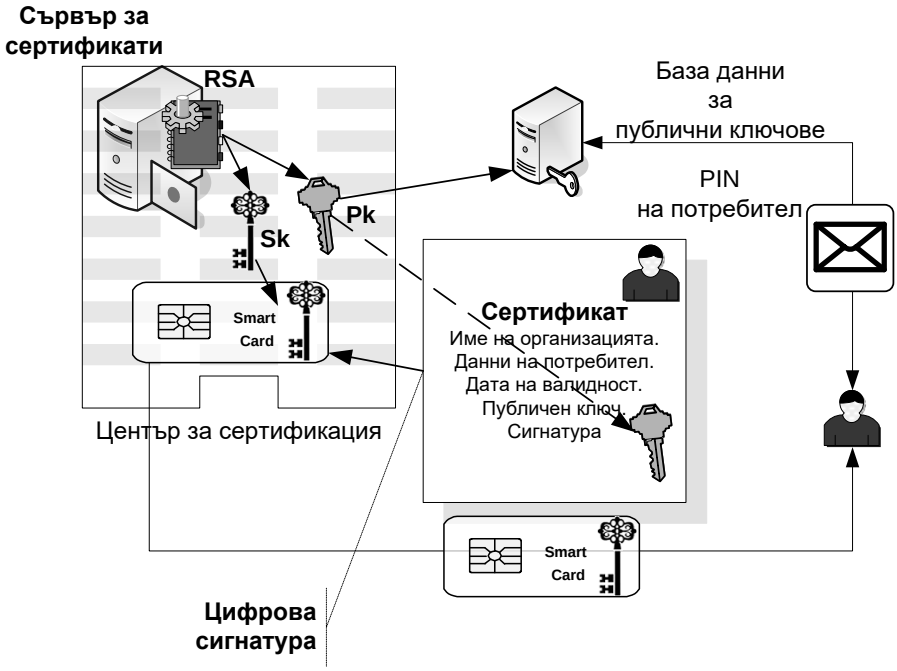
Базова дейност на сертифициращата организация е мениджмънтът на публичните и секретни ключове на потребителите. Мениджмънтът на ключовете съдържа:

- процедура за генериране на ключовете;
- създаване на архив;
- процедура за възстановяване на ключа;
- процедура за обновяване на ключа..

Генерирането на ключ може да се реализира по два начина: **централизирано** или **децентрализирано**.

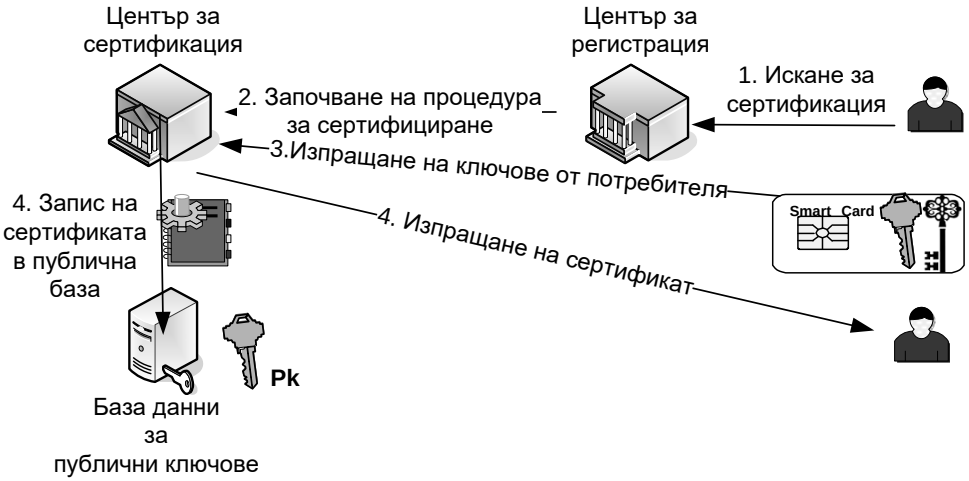
При централизираното генериране ключовете се създават в центъра за автентификация (CA – Certification Authority) и се включват в издавания сертификат. Сертификатът се записва в смарт-карта[8] (Фиг.11.2), която се предоставя на потребителя за да може да изпълнява криптиращи и декриптиращи процедури. Достъпът до тази смарт-карта се извършва посредством номер за персонална идентификация (Personal Identification Number - PIN).

[8] Възможно е и ползването на други носители.



Фиг.11.2 Централизирано генериране на ключове

При децентрализираното генериране на ключове (Фиг.11.3) се изпълнява следния алгоритъм:



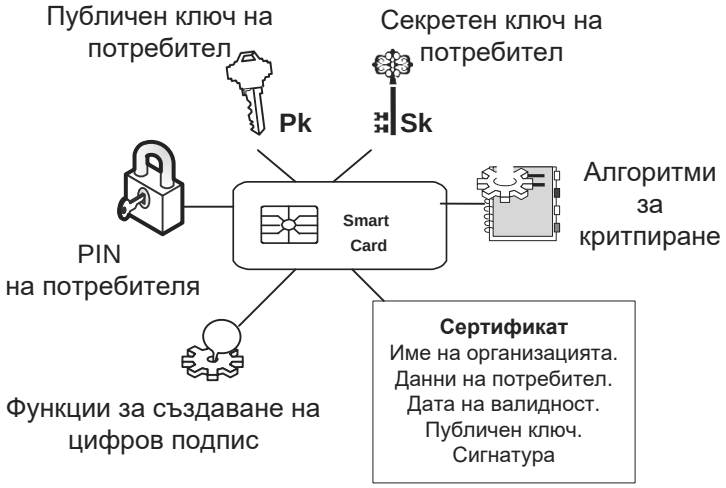
Фиг.11.3 Децентрализирано генериране на ключове.

1. Желаещият да получи сертификат подава заявка в центъра за регистрация (Registration Authority), където се удостоверява неговата самоличност.

2. След установяването на самоличността му, центърът за регистрация инициира процедура за издаване на сертификат. В процеса на протичане на процедурата се изисква потребителя да представи своите ключове.
3. Бъдещият собственик на сертификата предоставя ключовете, които той или трета страна са генерирали.
4. Получените ключове се изпращат в CA. CA генерира сертификат X 500, записва публичния ключ на собственика на сертификата в общо достъпна база данни, както и самия сертификат.

Центърът за регистрация (**Registration Authority**) е компания или организация, отговорна за идентификацията и автентификацията на сертифициращия се субект. Желаещите да получат цифров подпис подават документите си в такава организация. Организацията е длъжна да проучи клиента и да го идентифицира еднозначно. В процеса на идентифициране се изисква представянето на валидни държавни документи за удостоверяване на идентичността и установяване на контакт с лицето по начин, гарантиращ сигурността на връзката.

Надеждното съхраняване на сертификата и запазването на секретния ключ в тайна е от основно значение за валидността на сертификата. Единият от възможните начини за съхраняване на сертификатите е записването им в хардуерно преносимо устройство. Най-често това е смарт-карта или тампер. Удостоверяването на самоличността на притежателя се извършва на базата на парола (PIN[9]) или друг метод за идентификация[10]. На Фиг.11.4. е дадена схема, описваща съдържанието на смарт-карта за автентификация.



[9] Аналогично е действието на картите в GSM апаратите.
[10] Например използване на биометрия.

Фиг. 11.4 Смарт-карта съдържаща сертификат

11.3 ПРОТОКОЛИ ЗА КРИПТИРАНЕ, ИЗПОЛЗВАНИ В IP КОМУНИКАЦИОННИ СИСТЕМИ

11.3.1 Криптиране в мрежовия слой (Internet-протокол)

За да се реализира защита в Internet-протокол е необходимо да се въведе механизъм за криптиране на данните, пренасяни от дейтаграмата, и да се формира нова заглавна част. Новата заглавна част се съставя така, че да не позволява подмяна на адресите на изпращащата и получаващата страна. Въвеждането на криптиране и новата заглавна част дават възможност за създаване на нов протокол – сигурен Internet-протокол (IP security protocol, IPSec).

IPSec е ключова технология, поддържаща криптиран обмен на данни. Детайлното описание на IPsec е дадено в RFC 1825–1829. IPsec осигурява конфиденциалност и автентификация , както и защита на интегритета, и авторството[11] на предаваната информация.

Постигането на по-висока сигурност при използване на IPsec се базира на [43]:

- Модифицирана заглавна част, за осигуряване на автентификация на пакета (IP Authentication Header) и интегритет на данните за цялата дейтаграма.
- Криптиране и капсулиране на полезния товар (Encapsulating Security Payload), посредством дефинирани от потребителя алгоритми.
- Изпълнение на процедура по договаряне и секретен обмен на ключа (IKE, Internet Key Exchange).

За автентифициране на всяка дейтаграма се съставя нова заглавна част - **IP Authentication Header (AH),** която формира и нови правила за взаимодействие на хостове в мрежовия слой. Тези правила на практика формират нов протокол. Следователно AH е протокол за контрол на **интегритета на данните и автентификация** на IP дейтаграмите. Конфиденциалността на данните и опасността от трафичен анализ **не се защитават**. За осигуряване на защитата на данните се използва протокол ESP (Encapsulating Security Protocol).

За целите на автентификацията, протоколът AH добавя допълнителни данни към заглавната част на IP протокола. Тази автентифицираща информация се получава посредством калкулиране на уникална стойност на всички полета от IP дейтаграмата (заглавните части на протоколите и потребителските данни), които не се променят по време на транспортирането на данните през мрежата. Полетата и опциите, които се променят по време на транспорта, участват в процеса на калкулиране със стойност 0 (не се взимат в предвид).

---

[11] Non-repudiation

Необходимостта от създаването на нов протокол произтича от факта, че не всички крайни системи могат или желаят да използват по време на работата си услуги за автентификация или за контрол на интегритета на данните. **IPSec** е разработен за да не се променя структурата на IP дейтаграмата.

Автентификацията и контролът на интегритета използват различни алгоритми за криптиране и съответно - ключове. За спазване на правилата на отворения стандарт трябва да се даде възможност на различните потребители да използват различни варианти на тези алгоритми, т.е., да ги договарят помежду си, преди да започне процедурата по обмен на данни. За да се постигне тази съвместимост всеки потребител трябва да опише използваните от него средства и да ги изпрати към отсрещната страна. Описанието на използваните техники и стойности се нарича **асоциация по сигурност (Security Association - SA).** В SA се включват всички детайли, които са необходими на един участник в комуникационния процес (получилия дейтаграмата) за да комуникира по сигурен канал с изпращащия дейтаграмата. В SA се включва следната информация:

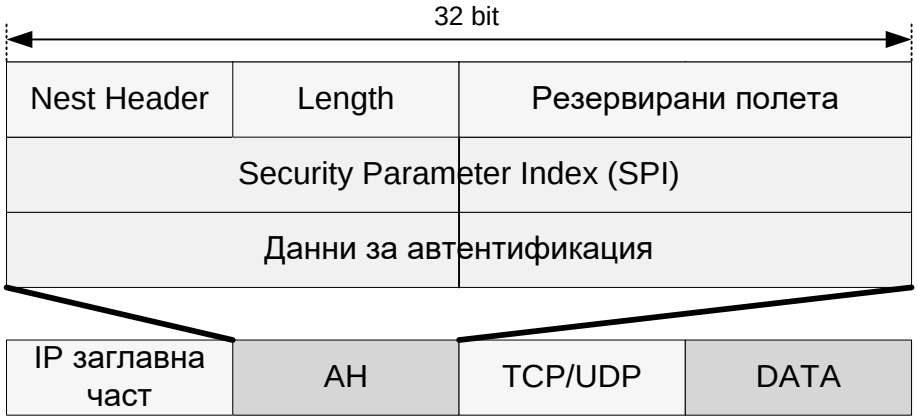
- режимът на работа на алгоритъма за автентификация и ключове за него;
- информация за криптиращи алгоритми, ключове за тях и честотата на промяна;
- информация за синхронизация на алгоритмите за криптиране;
- начинът за провеждане на автентификационна процедура;
- „времето за живот" на самото SA;
- IP адреса на създателя на SA.

SA представлява маркер[12] за дейтаграмата, по който тя може да се класифицира и обработва допълнително. **SA** се изчислява преди да се изпрати IP дейтаграмата от съответния хост. Всички SA, изпратени от един хост, са валидни само в едната посока на предаване. За обратната посока другия хост изчислява своето SA и го изпраща. В изчисляването на стойността на SA се включва и Destination Address[13] на получаващата страна.

Заглавната част на AH и начина и за разполагане в IP протокола е показана на Фиг.11.5.

[12] Допълнително вградена информация.

[13] IP адрес на компютъра, получаващ пакета.



Фиг. 11.5 Структура на IP Sec дейтаграма

Съдържанието на заглавната част на АН включва следните полета:
NEXT HEADER - 8 битово поле, идентифициращо местоположението на полезните данни, спрямо данните за автентификация.
PAYLOAD LENGTH – 8 битово поле, в което се записва дължината на данните за автентификация (Authentication Data) в брой 32 битови думи.
RESERVED – 16 битово поле, запазено за бъдеща употреба.
SECURITY PARAMETER INDEX (SPI) – 32 битово поле, което има псевдо-случайна стойност.
AUTHENTICATION DATA – дължината на това поле е променлива, но винаги се измерва в брой 32 битови думи. В него се записват необходимите данни за избрания конкретен метод за автентификация. В него влизат данни от алгоритми за създаване на цифрова сигнатура на дейтаграмата и данни за оформяне на асоциациите по сигурност (SA).

11.3.2 Протокол Encapsulating Security Payload (ESP)

ESP е протокол за гарантиране на сигурността и интегритета на потребителските данни (payload) в IP дейтаграмите. С него може да се реализира допълнително функция по автентификиация в зависимост от използваните криптиращи протоколи. За да се гарантира автентификацията на данните е задължително използването на АН заедно с ESP. ESP осигурява връзката между:

- хост и сигурен гейтуей или;
- сигурен гейтуей и друг сигурен гейтуей;

Сигурен гейтуей (security gateway) се нарича гейтуей, в който допълнително са инсталирани услуги за криптиране и протоколи за сигурен обмен на ключове за криптиращи алгоритми. Защитата от анализ на трафика и авторството[14] на данните не са обект на защита в този протокол.

[14] Non-repudiation

Полезният товар на ESP се състои от две части: блок от данни в явен вид и блок с криптирани данни. Явните данни съдържат информация за това, кои алгоритми за криптиране са използвани. Тази информация се използва от приемната страна с цел определяне на криптографския алгоритъм, с който да декриптират доставените с тази дейтаграма данни. Блокът с криптирани данни съдържа потребителските данни, получени от протоколите от горните слоеве и техните заглавни части.

Първият блок се състои от две части:

- **Security Parameter Index (SPI)** представлява 32 битов номер, информиращ получаващата страна какви алгоритми за криптиране са използвани от изпращащата страна, как да се получи информация за ключовете и каква е валидността на ключовете по отношение на времето.
- **Sequence Number –** представлява номер, които отчита за кой пореден път е бил използван един и същ SPI-номер в рамките на една сесия. Целта на това броене е да се осигури защита от копиране на пакети.

Копирането на пакети е интрузия, която се базира на подслушване на мрежата с цел прихващане на определени пакети и повторното им изпращане по-късно. При повторно изпращане на копиран пакет получаващата страна има възможност да сравни получения Sequence Number с останалите получени номера за рамките на сесията. При съвпадение получения пакет се отхвърля.

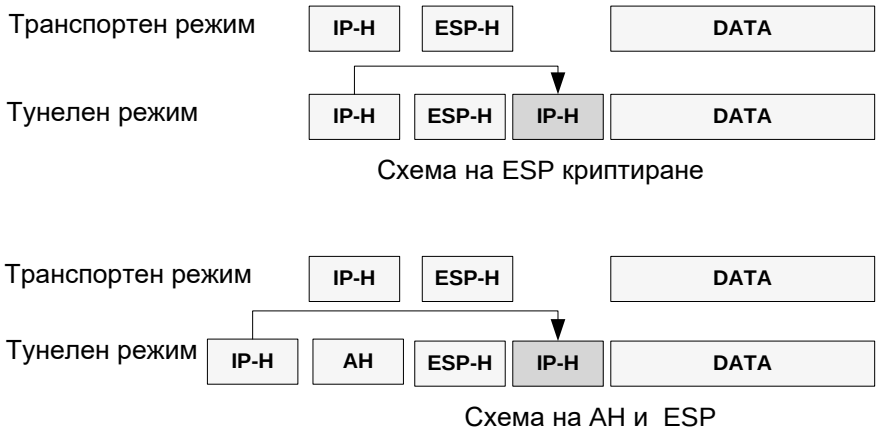
В края на ESP са добавя и AH, ако е използван.

ESP може да работи в два режима на работа: *тунелен* режим и *транспортен* режим.

Тунелният режим на работа на ESP осигурява криптиране на цялата IP дейтаграма. От криптираната дейтаграма се формира нова, в заглавната част на която се записва нов адрес на получателя и източника. По този начин се осигурява възможността дейтаграмата да бъде маршрутизирана през съответната комуникационна система.

При използване на **транспортен режим,** заглавната част на ESP се включва непосредствено преди заглавната част на протокола от по-горния слой (например преди заглавната част на TCP).

Формирането на IP дейтаграмите в двата режима на работа на ESP е представено на *Фиг.11.6* [43]



Фиг.11.6. Режими на работа на IP Sec

Със стрелки е показано мястото на действителната заглавна част на IP дейтаграмата. Въз основа на архитектурата за сигурност на Интернет протокола се изграждат цялостни решения за защита на данните от край до край при предаването им през несигурни публични мрежи. Тези решения се наричат **виртуални частни мрежи.**

11.4 ВИРТУАЛНИ ЧАСТНИ МРЕЖИ

11.4.1 Общи сведения и протоколи

Виртуалните частни мрежи (VPN - Virtual Private Network) *са предназначени да изграждат сигурни комуникационни канали между предварително дефинирани крайни системи (хостове) или компютърни мрежи.* Понятието „виртуална мрежа" трябва да се разглежда като логическо ниво на сигурност в дадена публична комуникационна система.

Преди разработването на технологията „виртуална мрежа" ресурсите на основната локална мрежа са ползвани чрез модем и отдалечен достъп през публична или наета телефонна линия.

В процеса на работа на дадена корпорация се налага даден потребител да пътува извън физическите рамки на защитената корпоративна мрежа. За да може да ползва нейните ресурси, той се нуждае от метод за тяхното ползване. Такъв метод се нарича **отдалечен достъп**. Отдалеченият достъп (Remote Access) дава възможност за използване на данни и ресурси от членове на корпоративната мрежа, намиращи се **извън зоната на сигурност**[15].

Използването на VPN намалява стойността за изграждането на връзката, увеличава броя на мобилните потребители, които могат да бъдат обслужени, и

[15] Понятието е определено в при разглеждането на защитните стени.

повишава качеството и сигурността на самата връзка. Отделният потребител следва да има единствено мрежов интерфейс за достъп до IP базирана мрежа. VPN се изгражда чрез технологията „клиент-сървър".

VPN клиент се нарича *хостът, инициращ връзка с VPN сървъра*.

VPN сървър се нарича *автентифициращата система, която определя какви протоколи за криптиране да се използват за осигуряване на сигурността на комуникационния канал*.

Използването на тази технология има за цел да осигури прозрачност на системата за сигурност по отношение на крайния потребител.

Възможните методи за изграждане на VPN са:

- изграждане на корпоративна виртуална мрежа;
- изграждане на виртуална мрежа с възможност за достъп от отдалечен потребител;
- изграждане на виртуална мрежа между двама или повече корпоративни партньори;
- изграждане на виртуална мрежа чрез тунелиране.

Изграждането на **корпоративна виртуална мрежа** се извършва в случаите на необходимост от защита на специфични данни в рамките на общата комуникационна мрежа за една организация.

За да се организира защитен обмен на данни между корпоративни партньори, те трябва да свържат мрежите си като гарантират сигурността на комуникацията помежду си. Изграждането на сигурни комуникации между корпорации-партньори се основава на използване на отворени стандарти за комуникации и използване на специализирани решения за сигурност за мрежата на всеки отделен партньор. Всяка компания може да изгради в рамките на локалната си мрежа собствена виртуална мрежа с която осигурява отдалечения достъп на служителите си до доверената си мрежа и гарантира прозрачен и сигурен достъп до мрежите на нейните партньори.

Маршрутизирането на пакетите в рамките на виртуалните мрежи, се осъществява на базата на т.нар. **тунелиране**. Тунелирането е технология за изграждане на сигурна комуникационна среда между външна мрежа или персонален компютър и доверена мрежа. То е свързано с капсулиране на пакетите от транспортния слой в IP пакети, и изпращането им по предварително договорени маршрути. За да се изгради тунел могат да се използват следните елементи:

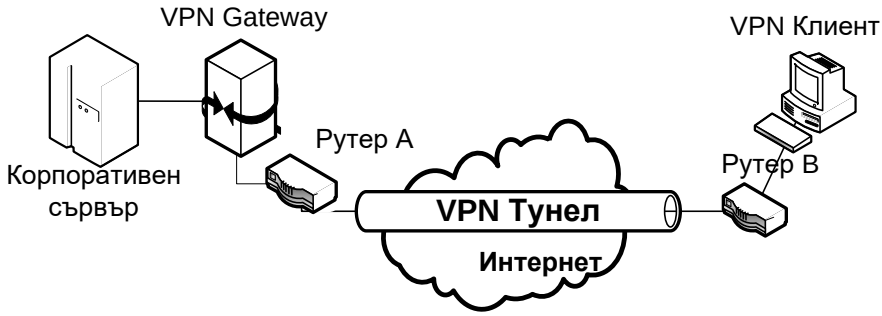
Тунелен протокол за връзка от тип точка-точка (Point to Point Tunneling Protocol, PPTP). Представлява разширение на класическия Point to Point Protocol (PPP). Протоколът PPP осигурява капсулиране на протоколите IP, IPX, или NetBEUI в IP пакети. Обикновено PPP се използва от доставчиците на Internet (ISP, Internet Service Provider) за осигуряване на връзка (тунел) от край до край между сървърите им.

Фиг .11.7 Изграждане на тунел между клиент и сървър

Протокол - Layer 2 Forwarding (L2F). Използва се за препредаване (тунелиране) на протоколи от по-високите слоеве към протоколите от каналния (Data-Link) слой. Трафикът, генериран от L2F, не е криптиран.

Протокол - Layer 2 Tunneling Protocol (L2TP). Този протокол е хибриден и съвместява функциите на Layer2Forwarding[16] протокол (L2F) и Point to Point Protocol[17]. Използва се за трансфер на трафик между мрежи, използващи различни технологии на пренос (например IP, SONET, ATM). Подобно на L2F, L2TP не може да дефинира механизъм за защита на данните от неоторизиран достъп. За да се гарантира сигурността на данните трябва да се използва IPSec протокол в IP комуникационни системи.

На Фиг11.8. е дадена схемата за свързване на хост към VPN мрежа.



Фиг. 11.8 Свързаване на хост към VPN мрежа

Тунелирането се изгражда на базата на маршрутизацията на пакетите между двата рутера А. За да се изгради мрежата е необходимо на отдалечена машина да се разположи специализиран софтуер, наречен VPN клиент. С помощта на този софтуер отдалечената крайна система се свързва до VPN гейтуея на своята доверена мрежа. След установяването на съединение (connection) отдалечената машина изпраща пакетите си в мрежата, без да

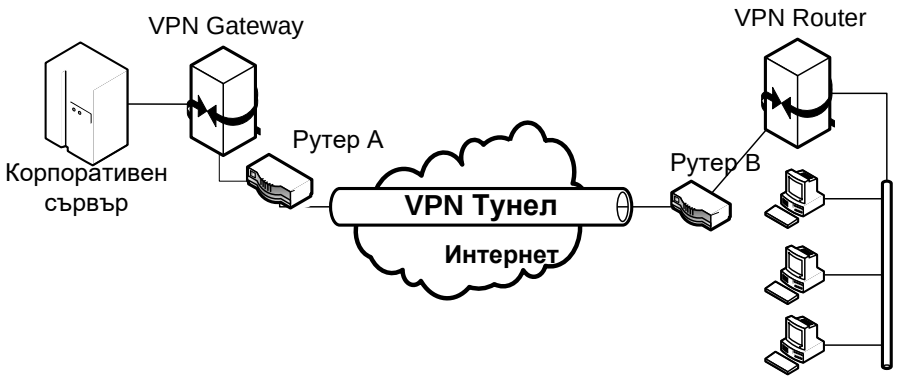
[16] Протокол на CISCO за изграждане на тунели в различни типове мрежи.

[17] Протокол от каналния слой, дефиниран в RFC 1661, 1662

предявява изисквания по отношение на сигурност към междинните Internet-провайдери.

11.4.2 Изграждане на VPN от тип Router-to-Router

Тази технология дава възможност за свързване на корпоративни мрежи между различни бизнес-партньори, имащи сходни системи. Тези системи формират крайните точки на тунелите. Вариант за такава реализация е показан на Фиг.11.9. Предимството при използване на такова решение е поддържането на множество от протоколи (например IP, IPX, NetBios) и възможността за установяване на множество съединения (connection) в рамките на един тунел. Криптирането и компресирането на данни може да се извършва както от рутера, така и в рамките на локалните доверени мрежи.



Фиг. 11.9 Свързване на корпоративни мрежи

11.5 ПРОТОКОЛ ЗА СИГУРНОСТ В ТРАНСПОРТНИЯ СЛОЙ SSL (SECURE SOCKET LAYER)

11.5.1. Общи сведения.

SSL протоколът е разработен за да предостави:

- сигурна криптирана връзка между две комуникиращи приложения (програми);
- механизъм за автентикацията им.

Този протокол използва принципа „клиент-сървър" и представя механизъм за двустранна автентификация. Идентификацията на сървъра, позволяваща на клиента да се убеди в достоверността му, се реализира чрез проверка на неговите сертификати и тяхната валидност При изискване от страна на сървъра, клиентът също трябва да се идентифицира , след което между двете страни може да се установи сигурна криптирана връзка.

SSL предоствя висока степен на защита на данните по време на предаването им по мрежата като непрекъснато следи за техния интегритет и

конфиденциалност. При детектиране на интрузия автоматично се прекъсва изградения комуникационен канал. За да осигури тези възможност SSL протокола включва в себе си три протокола:

- SSL протокол за запис (SSL Record Protocol);
- SSL протокол за договаряне (SSL Handshake Protocol);
- SSL протокол за допълнителни служебни съобщения SSL Alert Protocol, отговорен за обмяната на съобщения за грешки между двете комуникиращи страни.

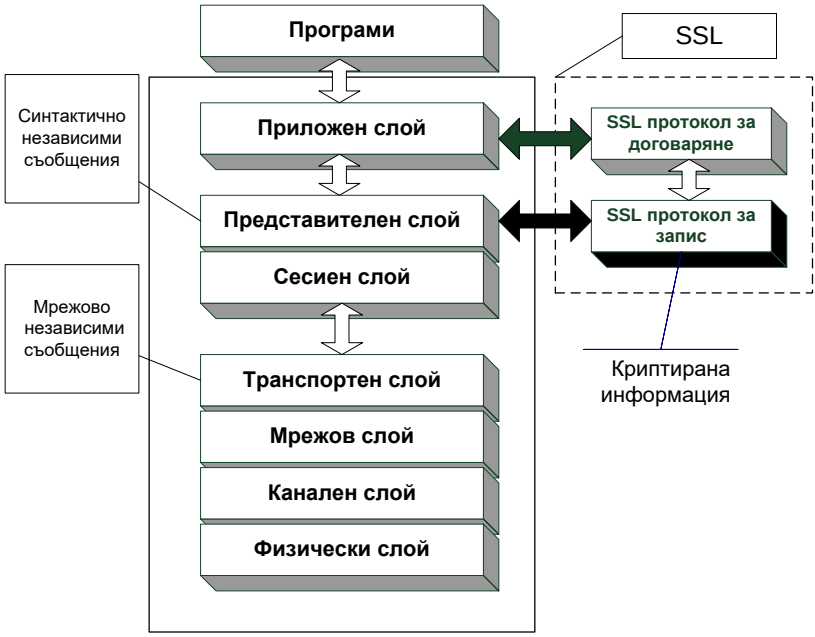
SSL протоколът за запис се използва за защитата на предаваните данни. За всяко съобщение, което трябва да бъде предадено, се извършва следната последователност от действия :

- фрагментиране на съобщението;
- компресиране на фрагментите;
- криптиране на компресираните фрагменти;
- предаването им към протокола от транспортния слой.

SSL протоколът за договаряне, използвайки протокола за запис, обменя серии от служебни съобщения между клиента и сървъра по време на изграждане на връзката. Целта на този обмена е:

- да се идентифицира сървъра пред клиента;
- да се позволи на клиента и сървъра да изберат криптографските алгоритми и ключове за предстоящата криптирана сесия;
- да се идентифицира клиентът пред сървъра (незадължително);
- да се стартира криптирана SSL връзка.

SSL е въведен в различни браузери и покрива всички услуги, подържани от тях (http, ftp, e-mail, news reader и др.). Криптиращите алгоритми за обмен на ключовете са **RSA** или **Diffie – Hellman.** Серификатите за цифров подпис са по стандарт **X.509**. За верификация на интегиртета на данните се използват хеш-функции SHA-1 и MD5.



Фигура 11.10 Местоположение на SSL

Протоколът за договаряне дава възможност на приложния софтуер да договори изграждането на сигурна сесия, а протоколът за запис реализира криптирания обмен на данните и ги предава към представителния слой. В представителния слой се определя как да бъдат форматирани данните, преди изпращането им към долните комуникационни нива.

На основата на тази схема на работа се осигурява криптирано предаване на информация от край до край (от програма до програма).

Използваните от SSL криптографски алгоритми са симетрични алгоритми и алгоритми с публичен ключ за цифрови подписи. Използва се и алгоритъма са краткото извлечение от съобщенията (код за автентикация на съобщенията: Message Authentication Code), който включва **HMAC за идентификация.** Прави се кратко извлечение на съобщението(хеш сума), което се праща към получателя. Той, от своя страна, го сравнява с това на изпращача. При съвпадение се гарантира интегритета на изпратените данни.

SSL версия 3.0[18] използва HMAC хеш алгоритъм за генериране на автентикациония код на съобщението. За да не се предава явен текст по линията, се извършва извлечение от явния текст, с което се инициализира генератор на данни (случайни числа).

Когато публичния ключ на сертификата не е продукт на трета страна[19], сървърът генерира временен публичен ключ, който се използва в процеса на

[18] Последната текуща версия на протокола към 2004г.

[19] Не е закупен от официална сертифицираща организация.

криптиране. Понеже генерирания временен ключ не е достатъчно сигурен, той трябва да бъде сменян достатъчно често.

11.5.2. Елементи на SSL.

SSL включва:

- **Метод за обмяна на ключа (Key Exchange Method**): SSL 3.0 поддържа избор на алгоритъма за обмяна, като може да бъде **RSA** или **Deffie-Hellman**[20] при използване на сертификат. Съобразена е и поддръжката на хардуерно оборудване[21] за обмяна на ключа**.**
- **Симетрични алгоритми за поточно криптиране:**
  - Без криптиране;
  - RC 4 със 40 битов ключ;
  - RC 4 със 128 битов ключ.
- **Симетрични алгоритми за блоково криптиране:**
  - RC 2 със 40 битов ключ;
  - DES 40, DES с 56 битов ключ, 3DES – DES с 168 битов ключ;
  - FORTEZZA при използване на FORTEZZA хардуер.

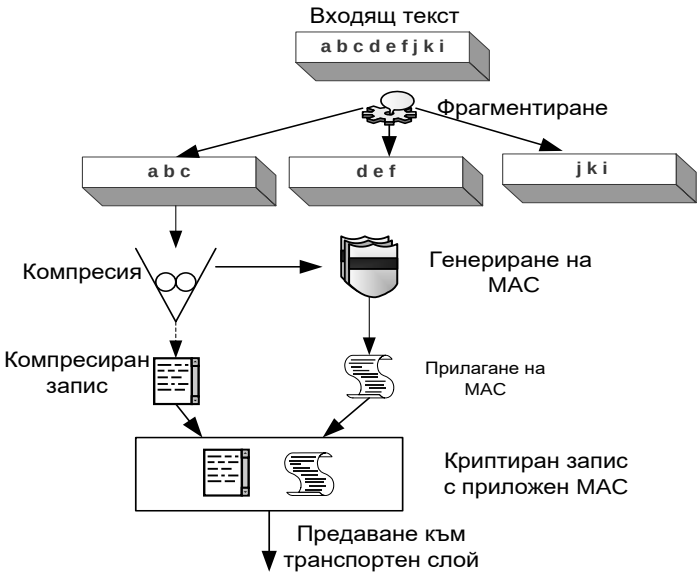
SSL протоколът получава данните от приложния слой, оформя ги в блокове, прилага компресия, изчислява съобщението за автентикация на данните, криптира и предава секретния текст на транспортния (**TCP**) протокол. При получаване на данните се извършват обратните процеси.

Изграждането на SSL сесия е показано на фиг. 11.12. Клиентът изпраща поздравително **ClientHello** съобщение, което е задължително за стартиране на процеса по договаряне на криптиращи алгоритми и ключове. В отговор сървърът изпраща свое съобщение. Освен стартиране на сесията, двете съобщения съдържат в себе си информация за версията на използвания SSL протокол, компресиращия алгоритъм, идентификацинния номер на сесията, списък с поддържаните криптиращи спецификации и обмяната на две случаини стойности извлечени от тази информация (**ClientHello.random** и **ServerHello.random)**.

---

[20] Подробно описание на алгоритъма е дадено в [31].

[21] Използване на допълнителна смарт карта с криптопроцесор.

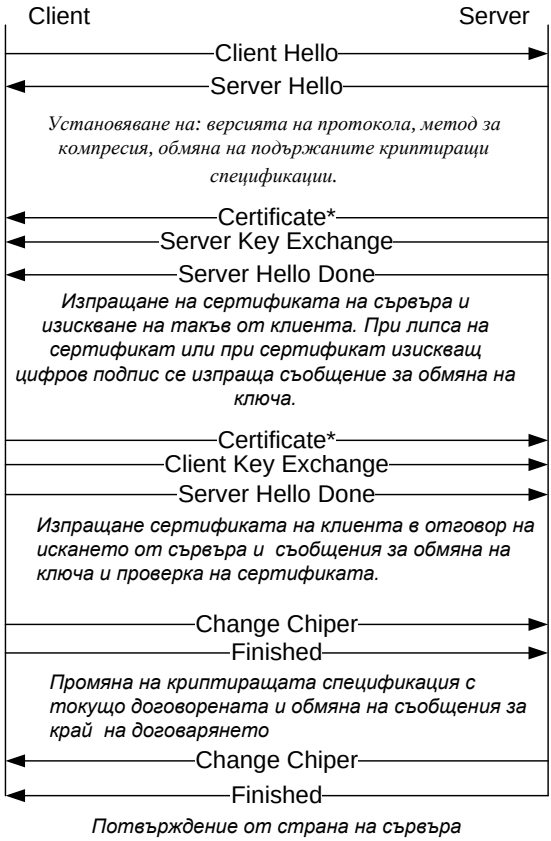


Фиг. 11.11. Защита на пакет в SSL

Следвайки **hello** съобщението, сървърът изпраща своя сертификат, за да бъде верифициран от клиента. Ако сървърът няма сертификат или сертификатът му е само за подпис, той изпраща съобщение за обмяна на ключа **ServerKeyExchange**. Следващото съобщение, което не е задължително, е съобщение за изискване на сертификат от страна на клиент. **CertificateRequest**, което е последвано от съобщение за приключване на първоначалното договаряне **ServerHelloDone.**

Ако сървърът е изпратил съобщение за изискване на сертификат от клиента, то клиентът е длъжен да изпрати съобщението за сертификат **Certificate** с парметър за типа или липсата на такъв (**no_certificate_alert**).След това се изпраща клиентското съобщение за обмяна на ключа **ClientKeyExchange,** чието съдържание ще зависи от избрания алгоритъм за публичен ключ, установен от предходните съобщения. Ако клиентът е изпратил сертификат с възможност за цифров подпис, се изпраща съобщение **CertificateVerify** за проверка на сертификата.

Съобщението за промяна на криптиращата спецификация **ChangeCipherSpec** се изпраща от клиента. Това стартира криптираща сесия за предаване на данни и приключва договарянето (съобщение **Finished)**. В отговор сървърът изпраща съобщение **ChangeCipherSpec,** с което декларира, че е приел договорената спецификация за криптиране, и изпраща свое съобщение **Finished** за край на договарянето. По време на предаване на данните може да се промени договорени криптиращ алгоритъм или ключ по допълнителен SSL протокол.



Фиг.11.12. Установяване на SSL сесия

КОНТРОЛНИ ВЪПРОСИ:

1. Защо е необходимо да се изгради публична криптографска инфраструктура?
2. Каква е разликата между център за регистриране и център за сертифициране?
3. Защо е необходимо да се ползва хардуерно устройство за съхраняване на цертификатите?
4. Как IPSec осигурява защита от атаките, свързани с подмяна на адреси и данни в мрежовия слой описани в глава 7?
5. Как SSL осигурява защита от атаките в мрежовия слой, описани в глава 7?
6. Опишете начина за подписване на писмо, изпращано с електронна поща. Какви технически и софтуерни средства е необходимо да притежавате? Направете им спецификация и определете приблизителната им финансова стойност.