

## ПРОТОКОЛҲО ВА СТАНДАРТҲОИ БЕХАТАРИИ ПАРДОХТҲОИ ЭЛЕКТРОНӢ

Ба механизмҳои ниҳоят бонуфуз ва афзалиятноки таъмини амнияти иттилоотӣ дар пардохтҳои электронӣ тавассути Интернет низомҳои зерин шомил мешаванд:



- протоколи SSL (Secure Socket Layer – протоколи васлкунии беҳавф), рамзгузори иттилооти тавассути Интернет ирсолшавандаро таъмин менамояд;
- стандарти SET (Secure Electronic Transactions – транзаксияи беҳавфи электронӣ), аз тарафи ширкатҳои маъруфи пардохтҳои электроники ҷаҳонӣ Visa ва MasterCard таҳия гардидааст ва харидуфурӯши беҳавф ва маҳрамонаро тариқи кортҳои пластикӣ таъмин менамояд.

Протоколи SSL, яке аз протоколҳои ниҳоят эътимодноки мубодилаи додаҳо ба ҳисоб рафта вазифаи рамзгузори иттилооти тавассути Интернет ирсолшавандаро иҷро менамояд. Стандарти SSL дар асоси низомҳои криптографӣ бо калидҳои кушод таъсис дода шудааст. Протоколи мазкур беҳатари иттилоотиро дар шабака тавассути протоколҳои TCP/IP ирсолшавандаро аз рӯи алгоритми рамзгузорӣ ва муайянкунӣ серверҳоро муштариён таъмин менамояд. Ин маънои онро дорад, ки қулли иттилооти бо барномаҳои браузер интиқолшаванда ва қабулшаванда рамзгузорӣ карда мешаванд. Аз суроғи URL сар карда, ҳамаи иттилооти ирсолшаванда, рақамҳои корти пластикӣ, маълумот оиди дастрасӣ ба сомонаҳои ҳифзшаванда (номи корбар ва рамзи дастрасӣ) ва инчунин иттилооти аз сервер ирсолшаванда низ рамзгузорӣ мешаванд.

Махфӣ будани пайғомҳо дар протоколи SSL тавассути

тадбиқи сохторҳои мувофиқати байниҳамдигарии додаҳо бо истифодабарии усулҳои криптографии тадбиқи калидҳои кушод ва симметрии таъмин карда мешаванд. Асоси бехатарии иттилоотиро дар ин протокол низомҳои криптографӣ бо калидҳои кушод ва симетрии ташкил мекунанд. Кулли бастаи пайғомҳо байни муштариён ва сервер бо ёрии калиди мавсимӣ рамзгузори мегардад, ки дар давраи аввали алоқамандии тарафҳо бо протоколи SSL, ки номи *handshake* (дастфишорӣ)–ро дорад, амалӣ мешавад. Рамзгузори бастаи додаҳо имконият медиҳад, ки мазмуни пайғомҳо ҳатто ҳангоми дастрасии нобакорони шабакавӣ низ махфӣ нигоҳ дошта шавад.

Беталафӣ ва комилии пайғомҳоро дар шабака имзои электронӣ таъмин менамояд.

Муайянкунӣ ё аутентификатсия<sup>1</sup> шахсияти байни ҳамдигарии фурӯшанда ва муштарӣ ба муштарӣ имконият медиҳад, ки тавассути пайвастшавӣ ба сервери зарурии транзаксия боварӣ ҳосил намояд ва сервер бошад дар навбати худ, ҳангоми зарурат эътимоднокии муштариро муайян менамояд.

Протоколи SSL танҳо як қисми масъалаҳои амниятиро ҳал карда метавонаду ҳалос. Саҳми протоколи SSL асосан дар таъминоти раванди рамзгузори иттилооти ирсолшаванда маҳдуд мешавад. Бинобар ин, барои ҳалли комплекси масъалаҳои дар боло қайд кардашудаи амнияти иттилоотӣ маҷмӯи протоколҳо ва хусусиятҳои зиёд таҳия гардиданд, ки яке аз низомҳои муваффақ ин баҳрабардорӣ аз стандарти SET мебошад.

Қайд кардан мумкин аст, ки стандарти SET расман дар рӯзи 1 феввали соли 1996-ум тавлид шудааст. Маҳз дар ҳамин рӯз ширкатҳои бонуфузи байналмилалии *Visa International* ва *MasterCard International* якҷоя бо як қатор ширкатҳои технологӣ дар бораи коркарди стандарти кушода ва ягона дар амнияти пардохтҳои электронӣ тавассути Интернет бо истифодаи кортҳои пластикӣ ба

---

<sup>1</sup> Authentication – шинохтагирифтани; муайянкунии асли шахсият; муайянкунӣ ва тасдиқи имзо. Раванди муайянкунии эътимоднокии тарафҳоро аутентификатсия мегӯянд.

ҳам омаданд.

Бо шарофати истифодабарии шаҳодатномаҳои электронӣ ва технологияи рамзгузории SET, ҳам ба фурӯшандаҳо ва ҳам ба истеъмолкунандагон имконияти муайянкунии кули иштирокчиёни харидуфурӯш пайдо мегардад. Ба ғайр аз ин, SET кафолати баланди ҳифзи рақамҳои кортҳои пластикӣ ва дигар иттилоотӣ маҳрамонро тавассути Интернет таъмин менамояд. Стандарти SET кушода буда, имконият медиҳад, ки таҳиякунандагони стандарт дар ҳалли масъалаҳои муштарак бо ҳам мувофиқат намоянд.

Дигар омили басо муҳими пешбарандаи технологияи SET ин истифодабарии низомҳои кортии мавҷуда ба ҳисоб меравад, ки кайҳо боз кортҳои пластикӣ ҳамчун афзори молиявӣ дар харидуфурӯшҳо мавриди баҳрабардории омма қарор дорад. Истифодабарии кортҳо технологияи мукамал буда, бо санадҳои ҳуқуқӣ мавриди ҷимояи қонуни кишвар қарор доранд.

Асоси низомҳои беҳатарии стандарти SET-ро алгоритмҳои криптографии стандарти DES (Data Encryption Standard – Стандарти рамзгузории додаҳо) ва RSA (Rivest, Shamir & Adleman encryption – рамзгузори бо усули Ривест, Шамир ва Адлеман) ташкил медиҳанд. Инфрасохтори SET дар мувофиқат бо инфрасохтори калидҳои кушода (PKI) сохта шудааст ва ба технологияи шаҳодатномаҳои электронӣ ҷавобгӯ буда, ба стандарти X.509-и ташкилоти байналмилалии стандартикунонӣ (ISO) мувофиқ мебошад. Хосияти асосии SET ин батартибдарории низомҳои таъминоти беҳатарӣ мебошад, ки аз тарафи низомҳои пардохтҳои байналмилалии гуногун пешниҳод мегарданд. Мувофиқи шартҳои пешниҳодкардаи ширкатҳои Visa ва Europa ба маркази амалиёти SET, стандарти мазкур бояд ба талаботҳои зерин ҷавобгӯ бошад:

1. талаботҳои маъмулӣ ва анъанавӣ ба амалиёт бо кортҳои пластикӣ иҷрошаванда, аз қабилҳои ҳифзи бино, назорати дастрасӣ, манбаи захиравии барқӣ, афзорҳои криптографӣ ва ғайра мебошанд;
2. истифодабарии хусусиятҳои иловагии экранҳои байншабакавӣ

(firewalls) барои ҳифзи хатҳои Интернет.

Чунин тарзи кор имконияти истифодабарии методикаи ягонаи баҳодихӣ ба тавакалро ҳангоми гузаронидани пардохтҳои электронӣ новобаста аз тарзи муайянкунии муштарӣ бо истифодабарии кортҳои анъанавӣ бо тасмаи магнитдор ё шаҳодатномаи электронӣ, муҳайё месозад. Чунин тарзи кор имконият медиҳад, ки иштирокчиёни системаҳои пардохтҳо ҳолатҳои мубоҳисавиро аз рӯи механизми мавҷуда ҳал намоянд ва тиҷорати электрониро дар ҳоли рушд қарор диҳанд.

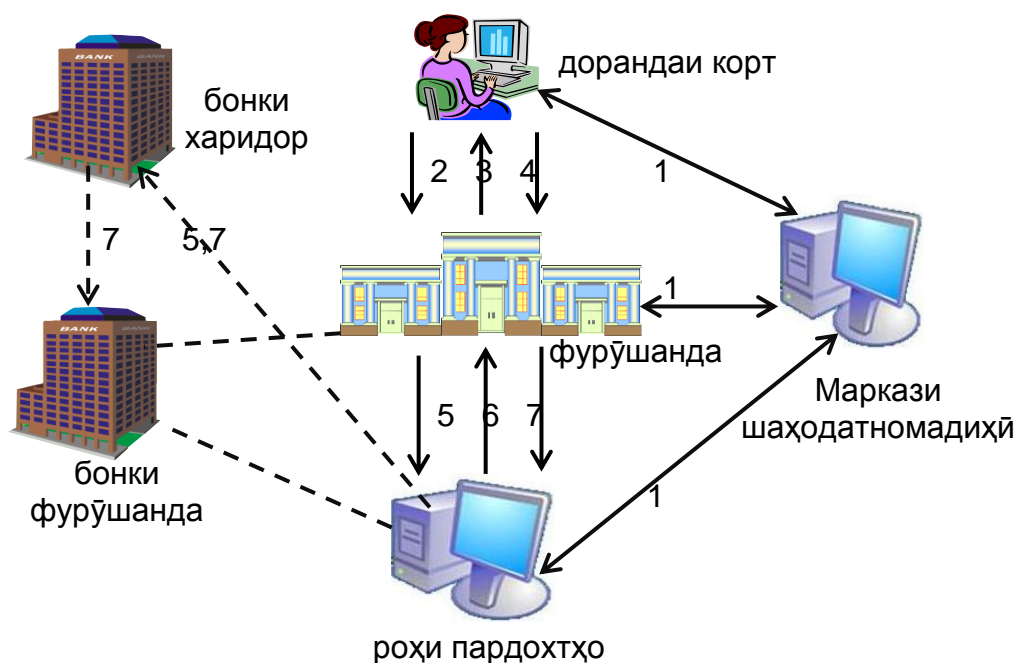
Стандарти SET имконият медиҳад, ки талаботҳои зерини дар мавриди бехатарии иттилоотии амалиёти тиҷорати электронӣ риоя шаванд:

- махфӣ нигоҳ доштани иттилоот оиди пардохтҳо ва фармоишот;
- сабт намудани иттилооти мушаххаси пардохтҳо тавассути имзои рақамӣ;
- криптографияи махсус бо калиди кушода барои гузаронидани санҷиши иштирокчиёни харидуфурӯш;
- муайянкунии соҳиби корди пластикӣ, тариқи имзои рақамӣ ва шаҳодатномаи корт;
- муайянкунии фурӯшанда ва имкониятҳои қабулкунӣ пардохтҳо бо кортҳои пластикӣ ва аниқ кардани имзои рақамӣ ва шаҳодатномаи электроникии фурӯшанда;
- омодагии пардохти транзаксияҳо баъд аз муайянкунии шаҳодатнома бо калиди кушода барои ҳамаи тарафҳо;
- бехатарии интиқоли иттилоот бо истифодабарии имкониятҳои криптографӣ.

Ҳоло кӯшиш мекунем раванди алоқамандии иштирокчиёни амалиёти пардохтҳоро муфассал дар мувофиқат бо хусусиятҳои SET дида бароем.

Иштирокчиёни сохтори алоқамандии пешниҳодгашта объектҳои зерин мебошанд:

- **дорандаи корт** - истеъмолкунанда, ки фармоиш медиҳад;
- **боники харидор** – сохтори молиявие мебошад, ки барои истеъмолкунанда корди пластикиро баровардааст;
- **фурӯшанда** – мағозаи электронӣ ё ширкати электроние мебошад, ки мол ва хизматрасониҳоро пешниҳод менамояд;
- **бонки фурӯшанда** – сохтори молиявие мебошад, ки ба хизматрасонии амалиётҳои фурӯшанда машғул мебошад;
- **роҳи пардохтҳо** (шлюзи пардохтҳо) – маъмулан ин системаи аз тарафи фурӯшанда мебошад ва бо бонки харидор дар алоқамандӣ кор мекунад;
- **ташкилоти шаҳодатномадиҳанда** – сохтори эътимодноке мебошад, ки вазифаи шаҳодатномадиҳӣ ва азназаргузаронии онро иҷро менамояд.



Сохтори алоқамандии иштирокчиёни низоми пардохтҳо тавассути стандарти SET

Алоқамандии иштирокчиёни амалиёт харидуфурӯши электронӣ дар расм оварда шудааст. Бо хати яклухт алоқамандии мувофиқи стандарти SET ва бо хати пунктир бошад баъзе амалиётҳои имконпазир ишора гардидаанд.

Тағйирёбии алоқамандӣ ва равандҳои иттилоотӣ дар мувофиқат

бо хусусиятҳои стандарти SET амалҳои зеринро дар бар мегиранд:

1. Иштирокчиён аз ташкилоти шаҳодатномадиҳӣ дархостнамуда соҳиби шаҳодатномаи электронӣ мешаванд;
2. Дорандаи корти пластикӣ рӯйхати маҳсулотҳо ва хизматрасониҳои мағозаи электрониро аз назар гузаронида, мол ё хизматрасониҳоро интихоб намуда, ба фурӯшанда фармоиш равон мекунад;
3. Фурӯшанда шаҳодатномаи электронию худро ба дорандаи корти пластикӣ ба сифати ҳуҷҷати тасдиқкунандаи эътимодноки, ирсол менамояд;
4. Дорандаи корти пластикӣ дар навбати худ ба фурӯшанда шаҳодатномаи электронию худро ирсол менамояд;
5. Фурӯшанда аз роҳи пардохтҳо иҷрокунии амалиёти санҷишро дархост мекунад. Роҳи пардохтҳо бошад иттилооти мавҷударо бо иттилооти бонки истехсолкунандаи корт муқоиса мекунад;
6. Баъди гузаронидани санҷиш роҳи пардохтҳо натиҷаи санҷишро ба фурӯшанда бармегардонад;
7. Баъди якчанд муддат фурӯшанда аз роҳи пардохтҳо иҷрокунии як ё якчанд амалиёти молиявиро талаб мекунад. Роҳи пардохтҳо бошад дар навбати худ аз бонки харидор ба бонки фурӯшанда гузаронидани маблағи муайяно талаб мекунад.

Эътимоднокии платформаҳои стандарти SET барои бехатарии пардохтҳои ташкилотҳо эътироф шудааст. Барои гирифтани иттилооти саҳеҳ оиди паҳнкунии стандарти SET, иттилоот оиди бонкҳо, шаҳодатномаҳои мавҷудаи ширкатҳои Visa ва Europay/MasterCard, ширкатҳои савдову хизматрасонии қабулкунандаи пардохтҳои SET аз сомонаи [set-sites.com](http://set-sites.com) ё сомонаҳои системаҳои пардохтҳои байналмилалӣ гирифтани мумкин аст.



#### **Саволҳо:**

1. Кадом протоколҳо ва стандартҳои амнияти иттилоотии шабакавино медонед?

2. Протоколи SSL кадом вазифаро иҷро мекунад?
3. Вазифаи стандарти SET аз чӣ иборат аст?
4. Талаботҳои стандарти SET кадоманд?
5. Иштирокчиёни сохтори алоқамандии харидуфурӯши электронӣ кадомҳоянд?

## 2.6. ТАЪМИНОТИ БЕХАТАРИИ ХАРИДУФУРҶШИ ЭЛЕКТРОНӢ

Харидуфурӯши маъмулии молу хизматрасониҳо ба ҷанбаи табиӣ асос ёфтааст. Одатан, дар мағозаҳои маъмулӣ муштарӣён кортҳои кредитӣ худро дар хариди маҳсулотҳо бемонета истифода мебаранд ва дар рафҳои он молро аз назар гузаронида даст мерасонанд, ламс мекунанд, дар бораи хусусиятҳои мол иттилооти пешниҳодшударо мутолиа намуда, оиди сифати молу хизматрасониҳои мағоза хулоса бароварда оиди харидорӣ намудан қарор қабул менамоянд. Бинобар сабаби мавҷуд набудани ин ҷанбаҳо дар Интернет ҳифзи тижорати электронӣ мушкилотҳо ва нозукиҳои худро дорад. Барои ҳифзи харидуфурӯш дар тижорати электронӣ қарорҳое қабул намудан лозим аст, ки хатар ва таваккалҳои зеринро бартараф намояд:

- **Тақлид ё имитатсия (Spoofing)** – қаллобон сомонаҳои содда ва тақлидшударо ба осонӣ имитатсия намуда, қалбакӣ месозанд ва бо ин роҳ моҳирона рақамҳои кортҳои кредитӣ ва дигар иттилоотӣ маҳфиро аз худ намуда бо мақсадҳои ғаразнокашон истифода мебаранд.
- **Ошкоркунии беиҷозат (unauthorized disclosure)** – ҳангоми иртиботи зинда дар харидуфурӯши молу хизматрасониҳо қаллобон метавонанд ба ин мубодила дастрасӣ пайдо намуда, иттилооти характери шахсидоштаро дузданд.

- **Амалҳои беиҷозат** – рақибон ё харидорони норозӣ метавонанд сомонии ширкати тиҷоратиро қорношоём гардонанд. Чунин амалҳо аксар ҳолат ба вайроншавӣ сомона оварда мерасонанд.
- **Ивазкунии иттилоот** – мазмуни иттилоот оиди харидуфурӯш ҳангоми иртибот тасодуфан ё қасдан иваз карда мешавад. Номии қорбарон, рақамҳои қортҳои қредитӣ ва қимати рақамҳои маблағҳои ирсолшаванда, ниҳоят иттилооти нозуқ ба ҳисоб мераванд.

**Ҳифзи сомона тавассути шаҳодатномаи рақамии VeriSign.**  
 Масъалаҳои дар боло овардашуда, аллақай ҳалли озмудашуда ва арзони худро пайдо намудаанд. Шаҳодатномаи рақамии ширкати VeriSign Server ID боварии соҳибқорони тамоми оламо соҳиб гардидааст, ки аз он дар тиҷорати электронӣ ва ҳифзи иттилооти маҳрамона хеле ҳам зиёд баҳрабардорӣ мешавад. Ҳолии ҳозир VeriSign теъдоди хеле зиёди Server ID дорад.

**Пешниҳоди тавсияҳо тавассути шаҳодатномаи рақамӣ.**  
 Шаҳодатномаи рақамӣ эквиваленти электронии литсензияи маъмулии фаъолияти соҳибқорӣ мебошад. Шаҳодатномаи электронӣ аз қониби сеюми салоҳиятдор СА (Certificate Authority) ҳамчун лоиқи боварӣ ба иштирокчиёни харидуфурӯши тиҷорати электронӣ дода мешавад. Ширкати VeriSign ба паҳнкунии шаҳодатномаҳои электронӣ дар тамоми олам машғул аст. Қониби вақолатдор, ки шаҳодатномаи электронӣ медиҳад, барои истифодабарии номи қорбар ва суроғии URL-и он кафил мешавад.

Пеш аз додани шаҳодатнома рақамӣ ширкати VeriSign тавсияҳои қорбар ё ширкатро омӯхта, санҷишҳои маҳсус мегузаронад. Дараҷаи эътимодноқиро дар тиҷорати электронӣ аниқ намуда, баъдан VeriSign ба қорбар ё ширкат шаҳодатномаи рақамӣ медиҳад, ки ба тавре тавсияи электронӣ дар эътимодноқии тиҷорати электронӣ ҳисоб мешавад. Шаҳодатномаи рақамӣ аз VeriSign ба ширкат боварии муштариёноро таъмин менамояд.



**Ҳифзи харидуфурӯши электронӣ бе харочотҳои иловагӣ.** Шаҳодатномаи рақамии VeriSign дар алоқамандӣ бо технологияи протоколи SSL кор мекунад, ки стандарти иртиботи беҳавф дар тамоми торнигор мебошад. Сервери торнигор метавонад бо шаҳодатномаи электронӣ кор кунад, агар ин шаҳодатномаро истехсолкунандагони ширкатҳои Apache Freeware, C2Net, IBM, Lotus, Netscape, Microsoft ё ширкатҳои дигар бароварда бошанд.

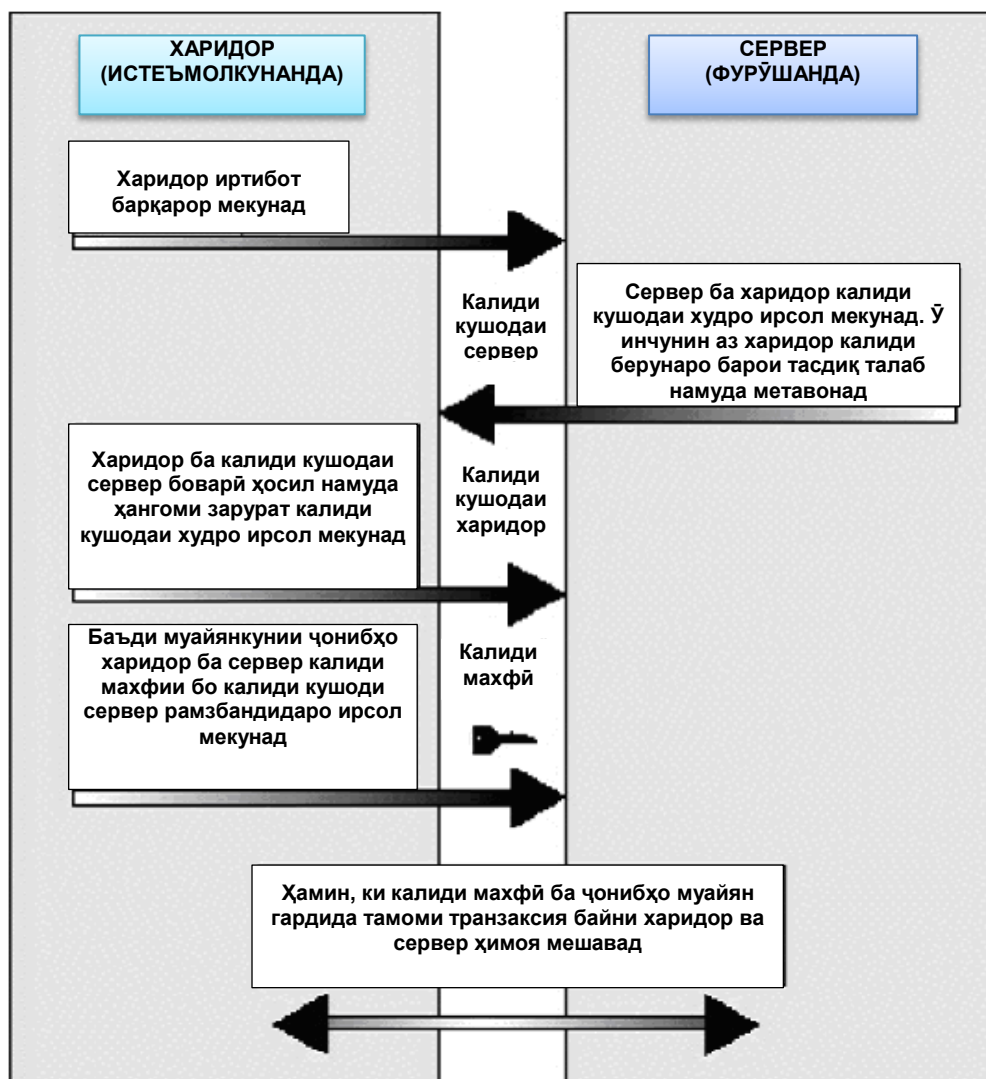
Баъд аз ҷойгиркардани шаҳодатномаи электронӣ дар сервери ширкати тиҷоратӣ ба таври худкор ҳимояи SSL фаъол мегардад, ки вазифаи он ташкил намудани ҳатти беҳавф байни ҷонибҳо дар тиҷорати электронӣ мебошад. Акнун сомонаи ширкат метавонад амн бо корбарони браузерҳои дилхоҳи Netscape Navigator, Microsoft Internet Explorer ва барномаҳои шинохташудаи почтаи электронӣ алоқамандӣ пайдо намояд. Баъд аз фаъолшавии шаҳодатномаи электронӣ, технологияи SSL дарҳол ба ширкат таъминоти қисматҳои зерини ниҳоят муҳими беҳатарии транзаксияҳоро ташкил мекунад:

- **Муайянкунии асл** – тавассути шаҳодатномаи электроники ширкати тиҷоратӣ, истеъмолкунанда асли будани ширкатро муайян ва аниқ намуда ба эътимоднокии сомона ва ширкати тиҷоратӣ боварӣ ҳосил менамояд. Баъдан истеъмолкунандагон бо боварӣ мол ва хизматрасониҳо фармоиш дода, иттилооти махфии тиҷорати худро ирсол карда метавонанд.
- **Пайғомҳои махфӣ** – технологияи протоколи SSL кулли иттилооти байни истеъмолкунанда ва фурӯшанда мубодилашавандаро рамзбандӣ намуда, калиди ягонро истифода менамояд. Барои таъмини беҳатарии иртибот истеъмолкунанда аз калиди мавсимӣ истифода намуда сервери фурӯшанда бошад тавассути калиди умумӣ рамзкушоӣ менамояд. Дар ҳар як иртибот ин калидҳо ҳамагӣ як маротибаги истифода мешавад. Чунин дараҷаи ҳифзи

иттилооти махфӣ кафолат медиҳад, ки иттилооти ба қаллобон дастрас гардида хонда нашавад.

- **Пайғомҳои мукамал** - ҳангоми ирсолкунии пайғом, ҳам компютери қабулкунанда ва ҳам компютери ирсолкунанда бо коди махсус иттилоотро генератсия мекунанд, ки ин раванд аз мазмуни пайғом асос ёфтааст. Агар ақаллан як симболи пайғом дар раванди табдилдиҳӣ иваз шавад, компютери қабулкунанда ин иттилоотро генератсия намекунад ва хабар медиҳад, ки пайғом беэтибор аст. Ҳамин тавр, ҳар ду ҷониб метавонанд ба пайғомҳои қабулнамудаашон боварӣ ҳосил намоянд.

Сохтори дар поён овардашуда раванди кафолати бехатарии транзаксияро байни сервери торнигори фурӯшанда ва истеъмолкунандаро кафолат диҳанд. Мубодилаи бо шаҳодатномаи рақамӣ алоқаманд буда дар лаҳзаҳои кӯтоҳтарин ба амал меоянд ва ба дахлати иловагӣ зарурат надорад.



Ширкати VeriSign ду намуди шаҳодатномаҳои рақамии гуногуни протоколи SSL-ро пешниҳод менамояд. Ҳар кадоми ин шаҳодатномаҳо дараҷаҳои мухталифи рамзгузорино вобаста аз версияи браузерӣ истифодашаванда пешниҳод намуда метавонанд.

Барои муайянсозии эътимоднокии ширкатҳо дар тижорати электронӣ ба таври пешфарз харидор эътимоднокии шаҳодатномаи электрониро санҷиш мегузаронад. Баъд аз санҷиш ва боварӣ бо ширкатҳо тавассути сервери торнигор пайвастанавии SSL-ро ташкил мешавад.

Амнияти иртибот дар тиҷорати электронӣ арзиши ниҳоят мӯҳим дорад. Таъмини амниятӣ ба амалиёти фаъоли бонкӣ, тиҷорати электронӣ ва дар маҷмӯъ кулли транзаксияҳо тадбиқ карда мешаванд



<b>Дархост ба SSL</b>	<b>Барқароркунии барномавии иртибот</b>	<b>Иртиботи ҳифзкардашуда</b>
<p>Корбар дар торнигор сомонаи ширкатро интихоб мекунад, ки суроғаи он тавассути протоколи https оғоз мешавад. Ҳарфи s истифодабарии протоколи SSL-ро ифода мекунад.</p>	<p>Браузери корбар ва сервери торнигор раванди мубодилаи иттилоотро, ки handshake ном дорад оғоз менамоянд. Сервер ба браузер калиди кушодаи худро пешниҳод менамояд, ки аз тарафи ширкатҳои эътимодноки VeriSign ё GeoTrust шаҳодатномаи рақамӣ дорад. Браузер дар навбати худ шаҳодатномати серверро месанҷад.</p>	<p>Мубодилаи иттилоот тавассути хатҳои ҳифзкардашуда амалӣ мешаванд, ки ба қаллобон имконият ҳалалдоркунии иртиботро маҳдуд менамояд. Санҷиши мукаммалии иттилоотро компьютерҳои ҳарду ҷониб генератсия менамоянд.</p>



### Саволҳо:

1. Кадом намуди хатар ва тавакалҳо дар тиҷорати электронӣ мавҷуданд?
2. Технологияи протоколи SSL ба ширкат таъминоти кадом қисматҳоро ташкил мекунад?
3. Сохтори раванди кафолати бехатарии транзаксияро шарҳ диҳед?