

# Universiteti AAB

## Lenda: Teknologjia elektronike Komerciale

### Ligjerata 5

Ky material eshte draft fillestar dhe si i tille mund te kete gabime eventuale

***Vërejtje:*** Përdorimi i paautorizuar i kësaj ligjërata do te mbrohet me ligj

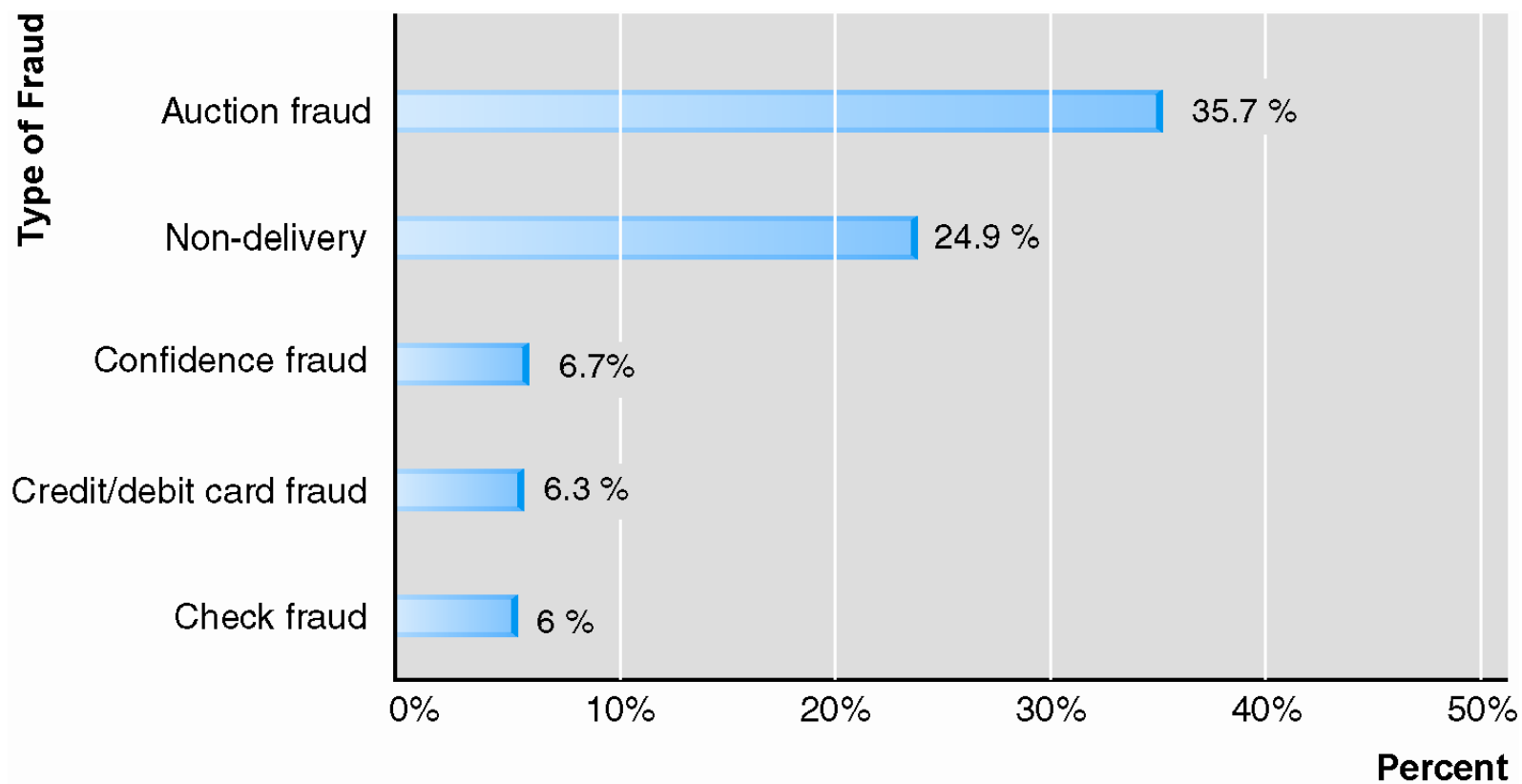
# Konceptet e pergjithshme te sigurise ne E commerce?

---

- Arritja e nivelit me te larte te sigurise
  - Teknologji te reja
  - Politika te sigurise dhe procedura te Organizatave te ndryshme
  - Standarde industriale dhe ligje qeveritare
- Faktoret tjere
  - Kostoja e sigurise vs. humbjet potenciale
  - Siguria shpesh “shperthen” ne hallkat me te dobeta

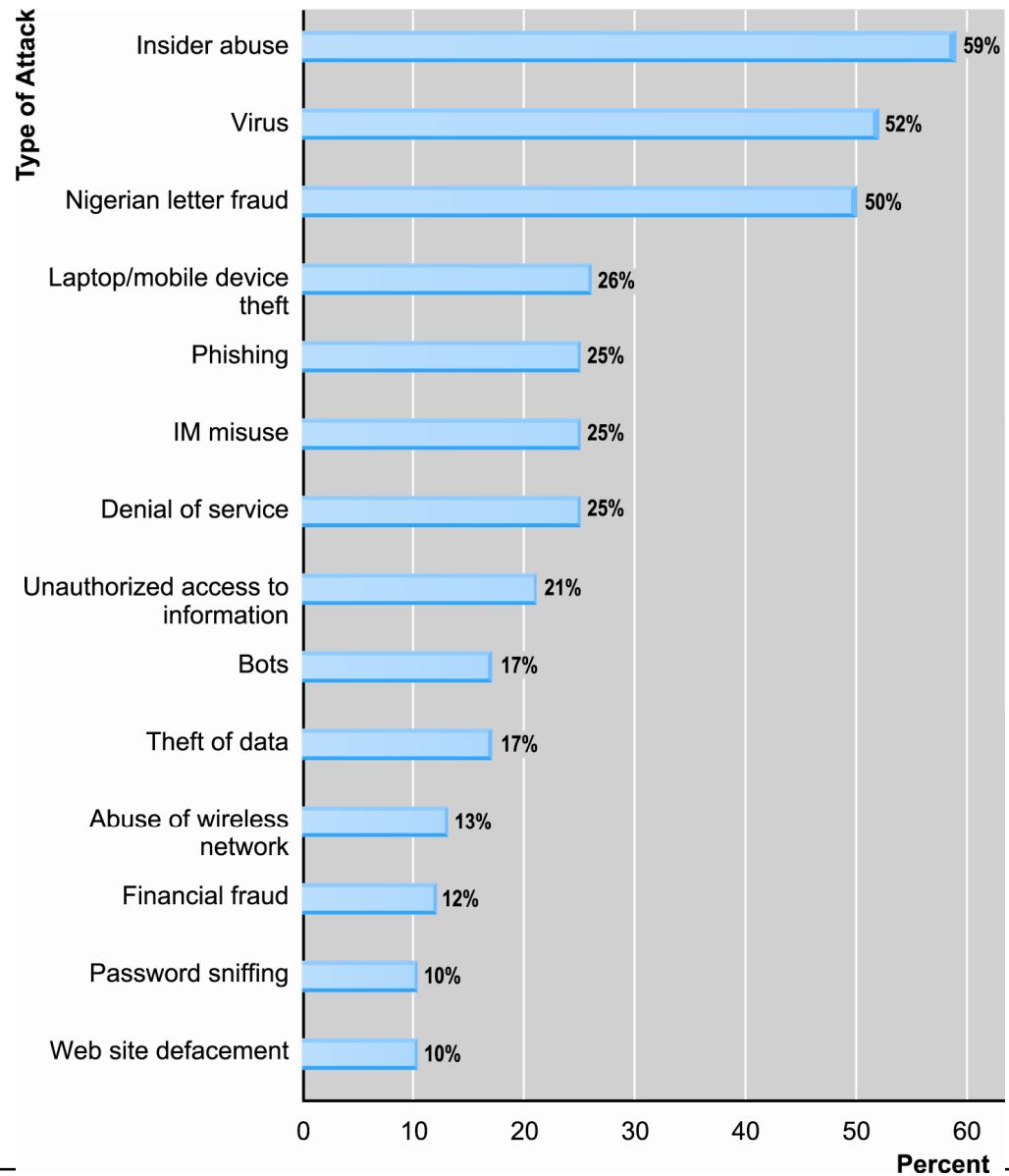
# Kategorite e krimeve ne internet

---



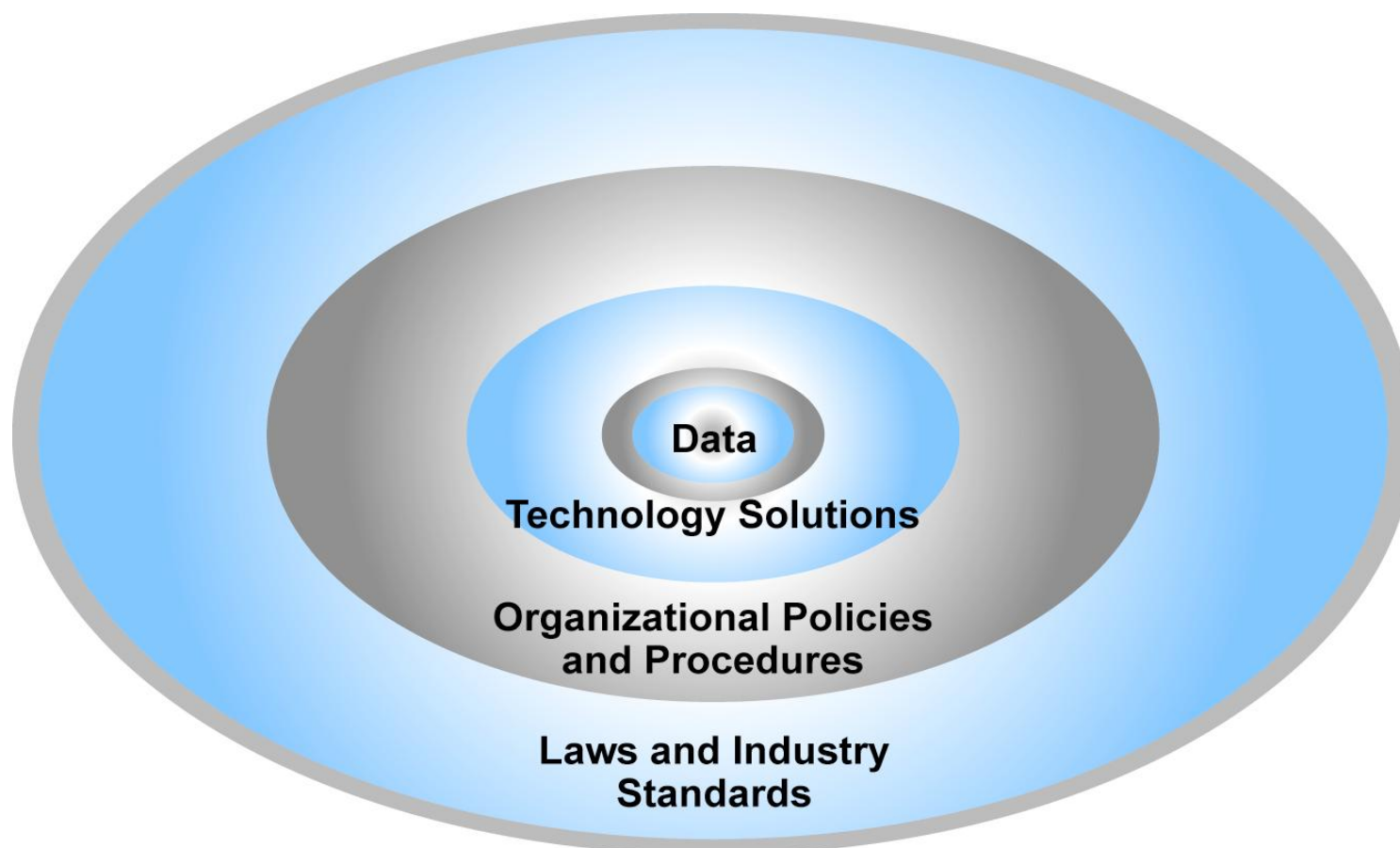
# Llojet e sulmeve kunder sistemeve kompjuterike

---



# Mjedisi i sigurise ne EC

---



# Siguria ne EC per nga perspektiva e konsumatorit dhe tregtarit

---

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

# Siguria dhe vlerat tjera!

---

- Siguria vs. perdorimi i lehte:
  - Sa me teper masa te sigurise qe shtohen, sajti behet me i veshtire per perdorim dhe behet edhe me i ngadalshem
- Siguria vs. deshira qe te veprohet ne menyre anonime
  - Perdorimi i teknologjise nga kriminelet per planifikimin e krimeve te ndryshme

# Kercenimet e sigurise ne nje mjedis EC

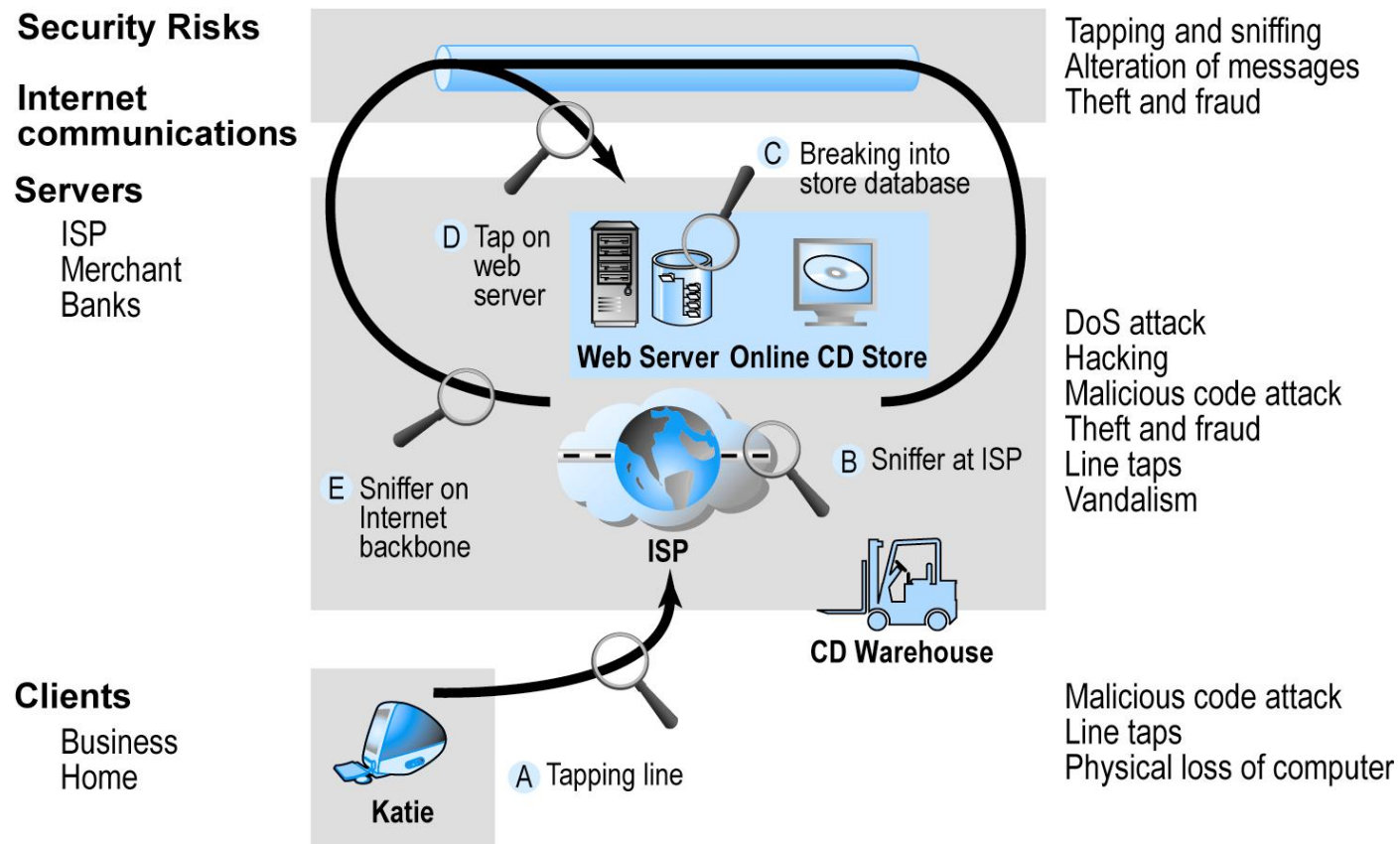
---

- Klient
- Server
- Kanalet komunikuese





# Pikat e dobeta ne nje mjedis EC



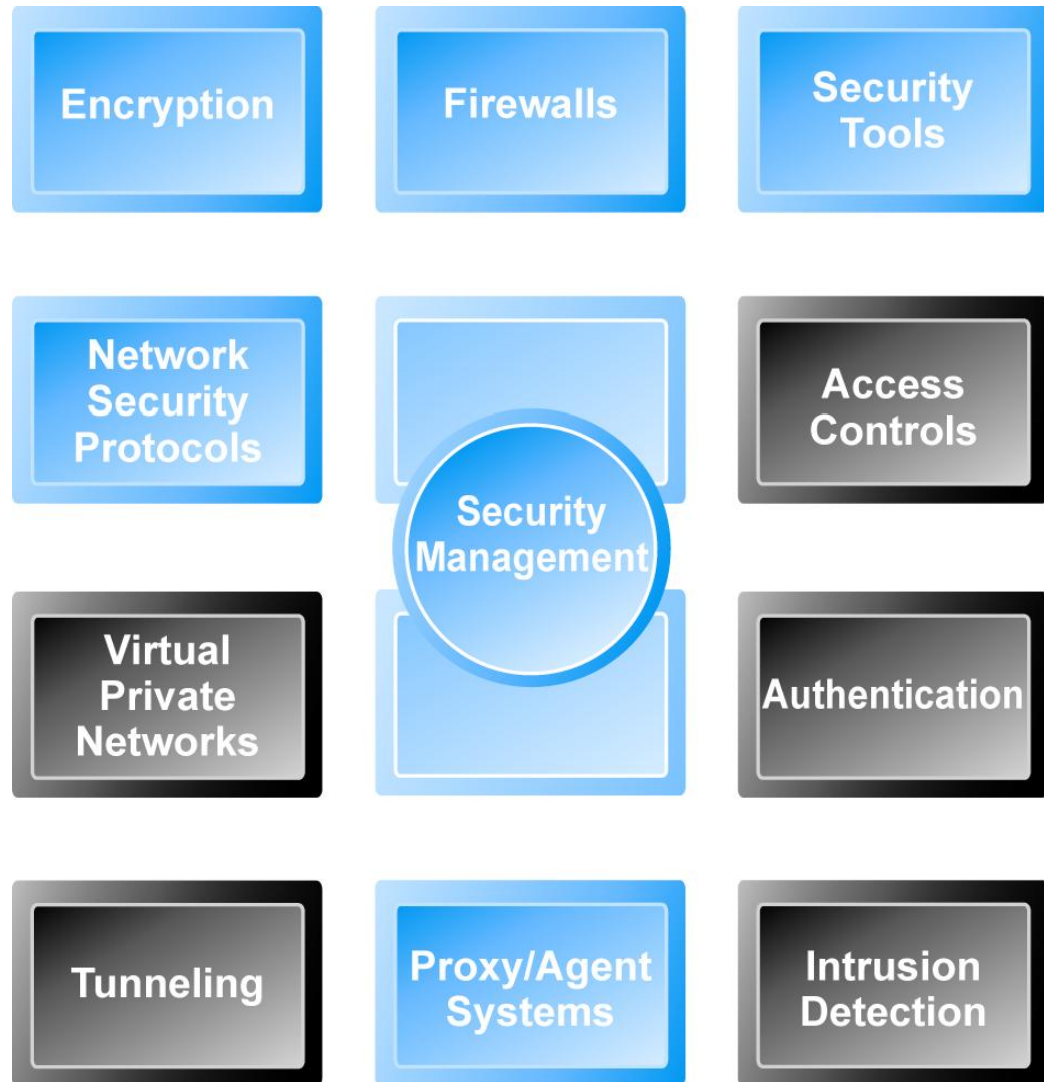
# Zgjidhjet teknologjike

---

- Mbrojtja e komunikimeve ne Internet (encryption)
- Siguria e kanaleve komunikuese (SSL, S-HTTP, VPNs)
- Mbrojtja e rrjetave (firewalls)
- Mbrojtja e servereve dhe klienteve

# Mjetet e nevojshme per te arritur sigurine ne nje sajt

---



# Mbrojtja e komunikimeve ne Internet: Enkriptimi

---

- Enkriptimi
  - Transformimi i tekstit te thjeshte, ne nje tekst te koduar qe nuk mund te lexohet nga askush, pos derguesit dhe pranuesit
  - Siguria e informatave te ruajtura dhe atyre qe transmetohen
  - Ofrohet:
    - Integritet i mesazheve
    - Autentifikim
    - Konfidencialitet

# Enkriptimi me çelës simetrik

---

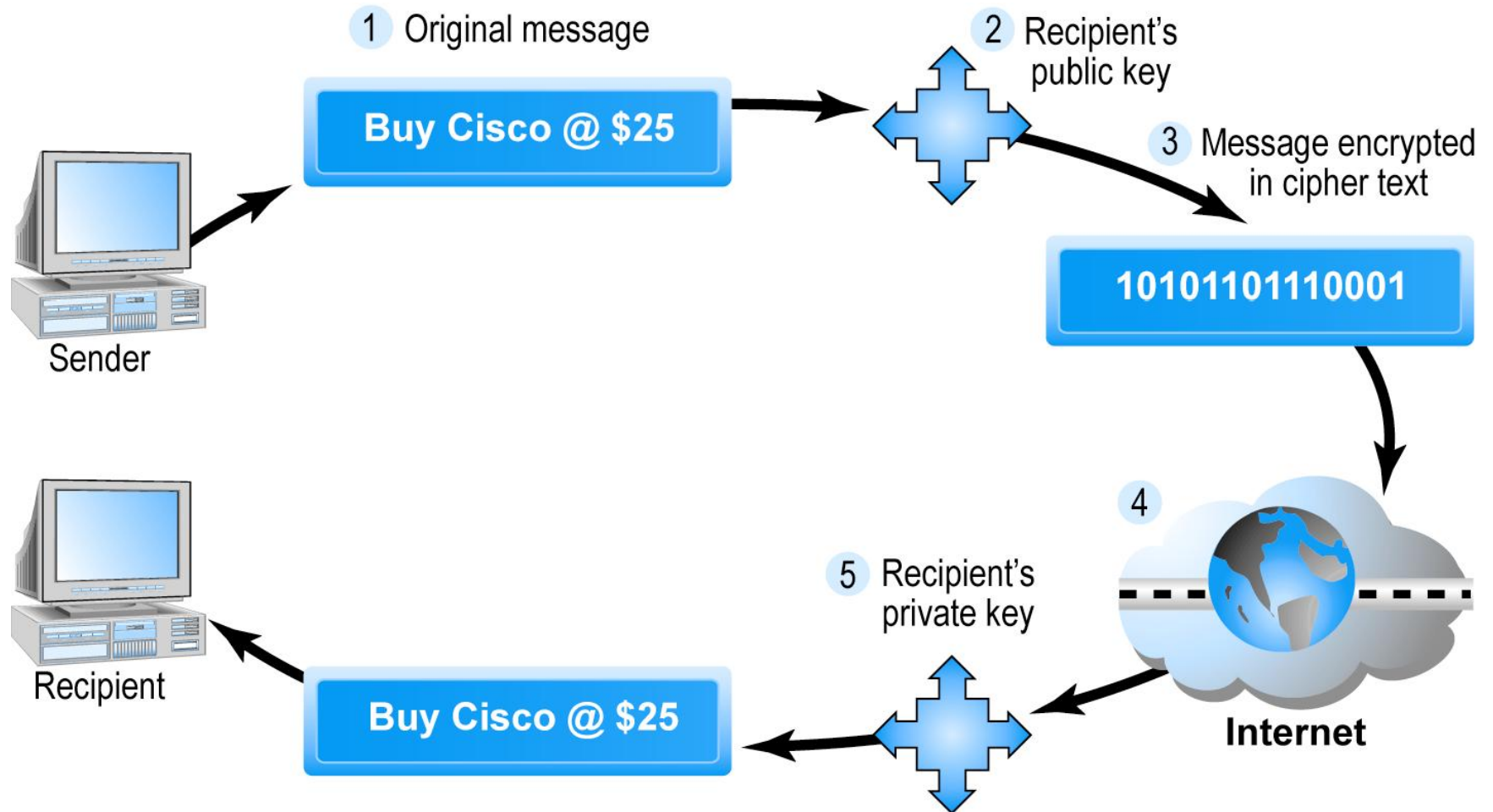
- I njohur gjithashtu si enkriptim me çelës sekret
- Derguesi dhe pranuesi e përdorin të njëjtin çelës digjital për enkriptimin dhe dekriptimin e mesazhit
- Kërkojnë çelësa të ndryshëm për secilin transaksion
- AES (Advanced Encryption Standard)
  - Enkriptimi më i përdorur me çelës simetrik
  - Përdor çelësa për enkriptim prej 128-, 192-, dhe 256-bit
- Standardet tjera përdorin çelësa deri në 2,048 bits

# Enkriptimi me çelës publik

---

- Përdor dy çelësa të nderlidhur matematikisht njëri me tjetrin
  - çelësin publik
  - çelësin privat (mbahet sekret nga zotëuesi)
- Të dy çelësat përdoren për enkriptim dhe dekriptim të mesazheve
- Kur njëri çelës përdoret për enkriptim të mesazhit, i njëjti nuk mund të përdoret për dekriptim të mesazhit
- Dërguesi e përdor çelësin publik të pranuesit për enkriptim të mesazhit; pranuesi përdor çelësin e tij privat për dekriptim të mesazhit

# Enkriptimi me çelës publik- shembull



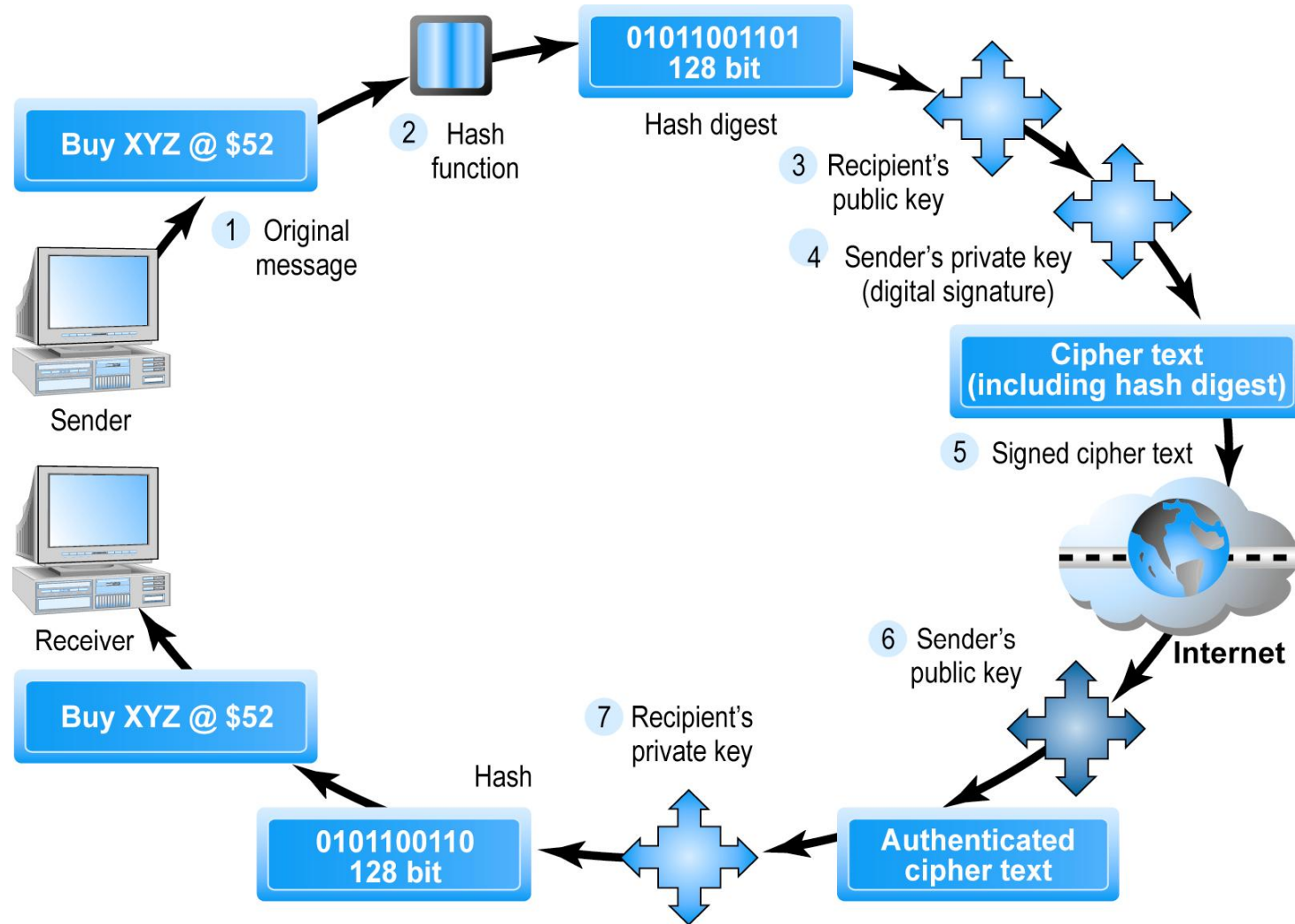


# Enkriptimi me çelës publik duke përdorur nënshkrimet digjitale dhe “Hash Digests”

---

- Hash funksioni:
  - Algoritem matematik që prodhon një numër të gjatë fikse që quhet mesazh ose “hash digest”
- “Hash digest” dhe mesazhi i enkriptuar me çelësin publik të pranuesit
- I tërë teksti i koduar më tej enkriptohet me çelësin privat të pranuesit – duke krijuar një nënshkrim digjital – për autenticitet.

# Kriptografia me çelës publik me nenshkrim digjital

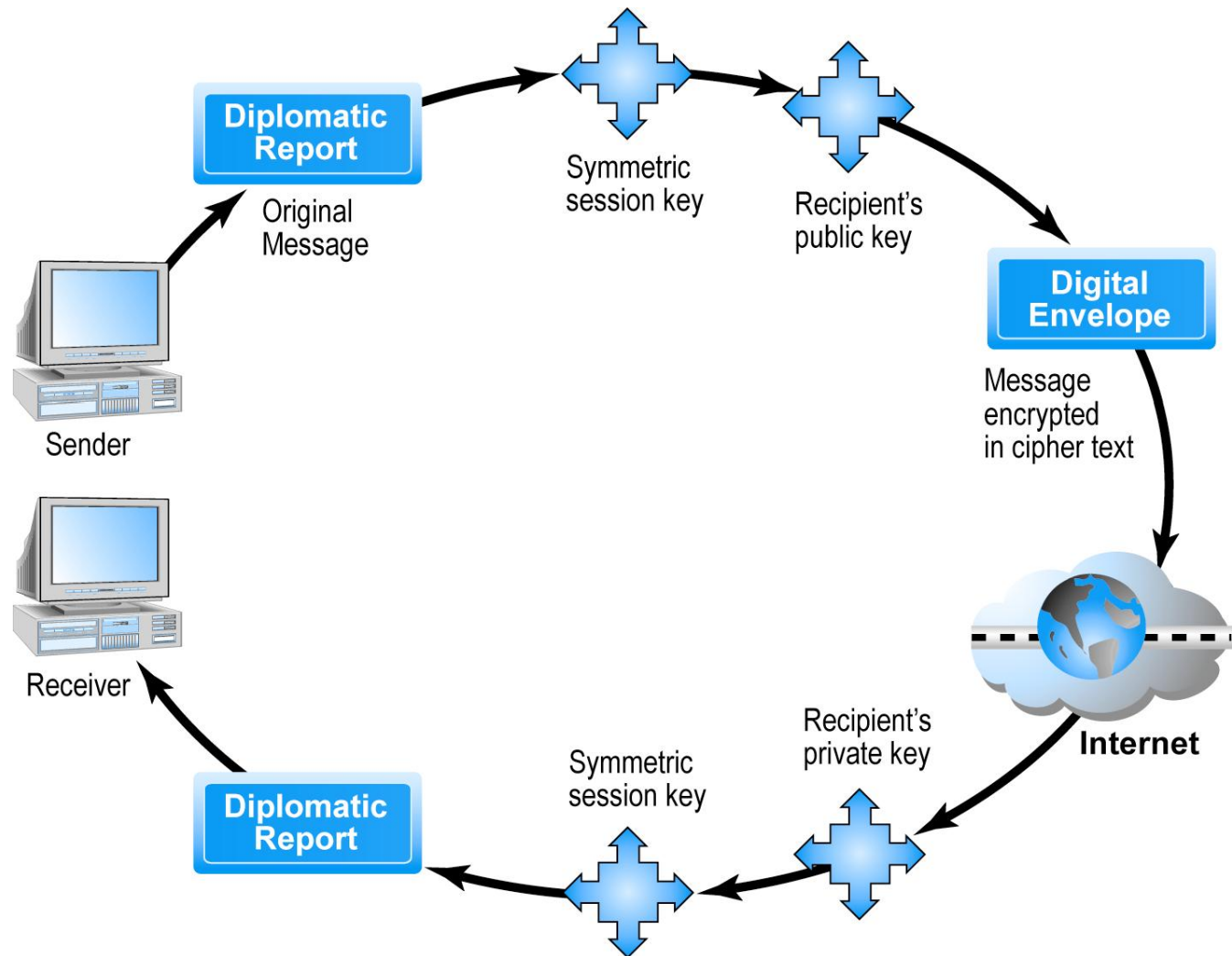


# Mbeshtjellesit digjital (Digital Envelopes)

---

- Adreson mangesite e enkriptimit me çelës publik dhe atij me çelës simetrik
- Perdor enkriptimin me çelës simetrik per enkriptimin e nje dokumenti, por perdor enkriptim me çelës publik per enkriptim dhe dergim te çelësit simetrik

# Krijimi i mbeshtjellesave digjital



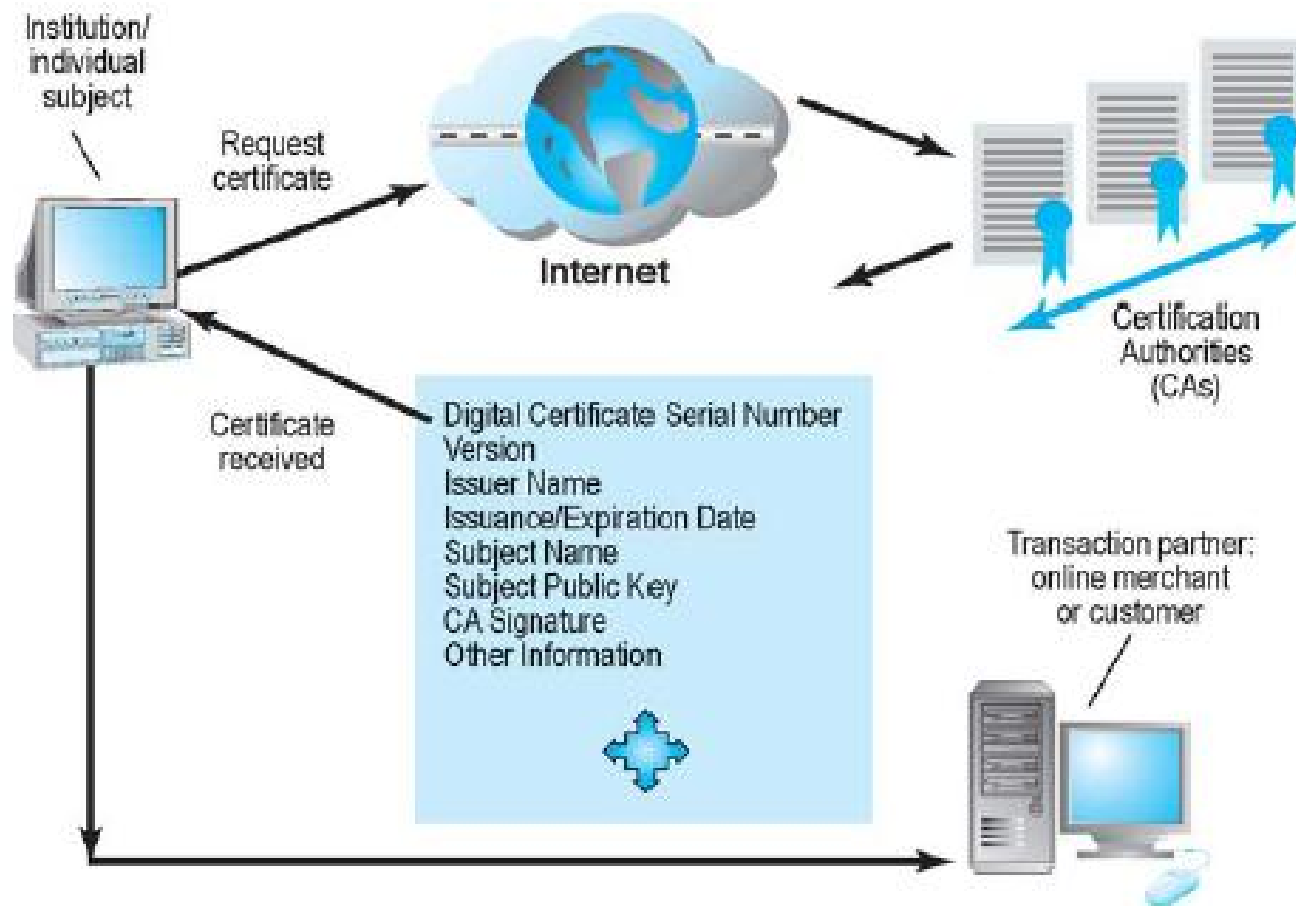
## Certifikatat digjitale dhe infrastruktura e çelësave publik (Digital Certificates and Public Key Infrastructure - PKI)

---

- Certifikatat digjitale perfshijne:
  - Emrin e kompanise
  - çelësin publik te nje subjekti
  - Numrin serik te nje certifikate
  - Daten e skadences, daten e leshimit
  - Nenshkrimin digjital te autoritetit per certifikim qe e leshon certifikaten
  - Informata tjera per identifikim
- PKI: CAs (Certificate Authorities) dhe procedurat e certifikatave digjitale qe pranohen nga te gjitha palet

# Certifikatat digjitale dhe autoritetet per certifikim

---



# Kufizimet qe ekzistojne ne teknikat e enkriptimit

---

- PKI (Public Key Infrastructure) aplikohet kryesisht per te mbrojtur mesazhet gjate transmetimit
- PKI nuk eshte efektive ndaj sulmeve te brendshme
- Nuk ka garanca qe nje kompjuter i verifikuar i nje tregtari te jete i sigurte
- CAs jane te parregulluara (unregulated), organizata te vet-zgjedhura

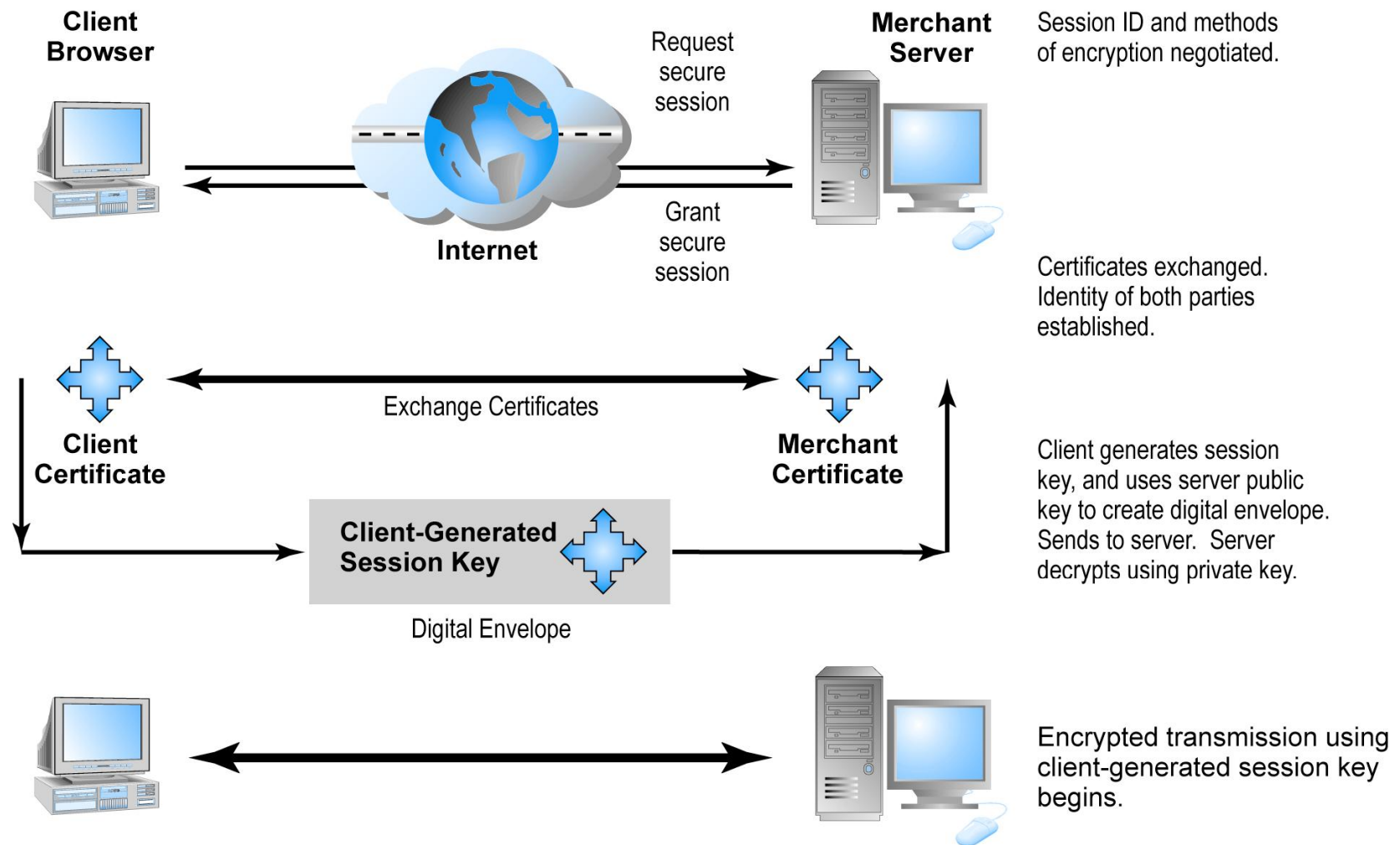
# Siguria e kanaleve komunikuese

---

- Secure Sockets Layer (SSL):
  - Krijon nje sesion te sigurte klient-server, ku URL e dokumentit te kerkuar, se bashku me permbajtjen, enkriptohen
- S-HTTP:
  - Ofron nje protokoll per siguri ne komunikim, qe eshte i dizajnuar per perdorim se bashku me HTTP
- Rrjetat virtuale private (VPN):
  - Lejon perdoruesit qe ndodhen ne largesi qe ti qasen ne menyre te sigurte rrjetit intern, permes internetit, duke perdorur protokollin PPTP (Point-to-Point Tunneling Protocol)



# Siguria e nje sesiioni duke perdorur SSL

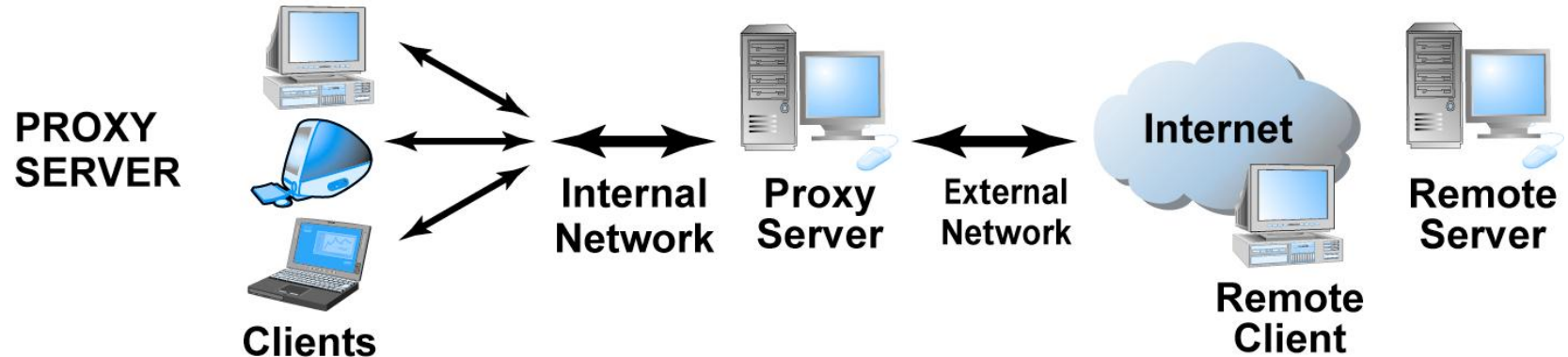
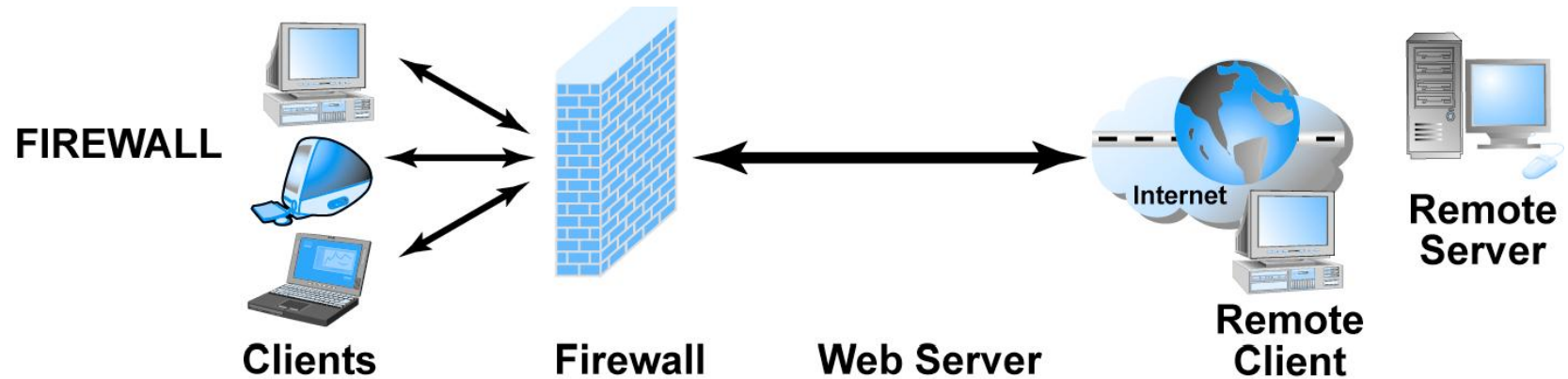


# Mbrojtja e rrjetave

---

- Firewall
  - Hradware ose softuer qe filtron paketat
  - Ndalon disa paketa qe te hyjne ne nje rrjet bazuar ne politikat e sigurise
- Proxy serveret (proxies)
  - Softuere qe trajtojne te gjitha komunikimet te drejtuara ne internet ose te marra nga interneti

# Muret mbrojtese dhe Proxy Serveret



# Mbrojtja e servereve dhe klienteve

---

- Kontrollat ne sistemin operativ:
  - Autentifikimi dhe mekanizmat e kontrollit te qasjes
- Softueri Anti Virus:
  - Menyra me e lehte dhe me pak e kushtueshme per parandalimin e kercenimeve
  - Kerkohen perditesime ne baza ditore

# Nenshkrimet digjitale

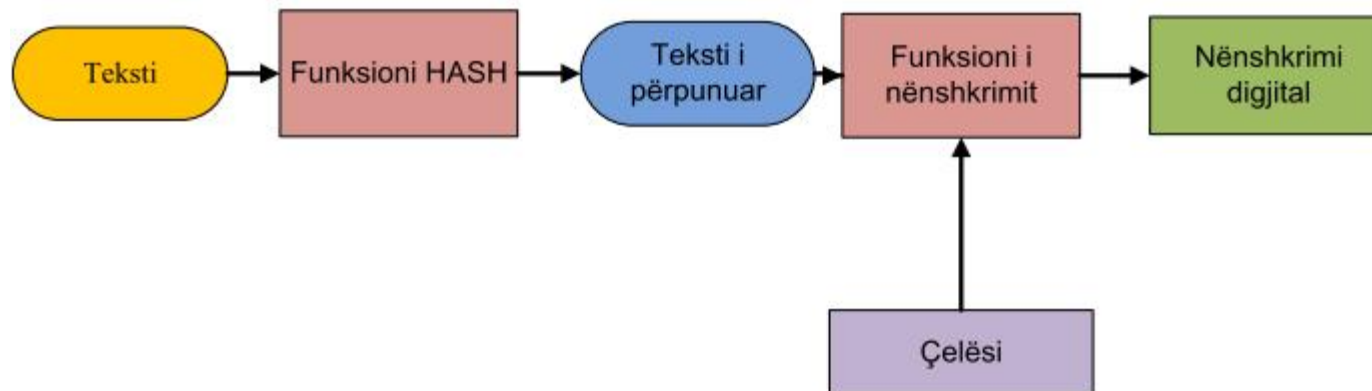
---

- Nenshkrimet digjitale jane nje nga zbulimet me moderne te kriptografise
- Qellimi eshte qe ti mundesohet nje perdoruesi te caktuar te nenshkruaje nje mesazh ashtuqe adresat e destinuar te mund ta verifikojne nenshkrimin.
- Nëse të dhënat apo nënshkrimi modifikohen ose ndryshohen, verifikimi i nënshkrimit do të dështojë.

# Nenshkrimet digjitale

---

- Nenshkrimi digjital është një metodë për enkriptimin e mesazheve (siç janë dokumentet, kontratat, shpalljet) që do të transferohen, duke e adoptuar protokollin për shkëmbim të të dhënave dhe algoritmin për enkriptim të të dhënave.
- Në këtë proces fitohet një abstrakt i cili duket si nenshkrim ose vulë që mund të përdoret nga pranuesi për verifikimin e identitetit të dërguesit.



# Funksionet e nënshkrimit digjital

---

- Funksionet e nënshkrimit digjital janë:
  1. Ruajtja e integritetit të të dhënave. Pasi që mesazhi të ndryshojë pak, abstrakti do të ndryshojë shumë për funksionet hash, ashtu që do ta shmang prishjen apo ndryshimin e mesazhit.
  2. Anti-refuzues: Duke përdorur algoritmin për enkriptim me çelës publik, dërguesi nuk mund të refuzojë se ai e ka dërguar mesazhin për të cilin e ka çelësin privat.
  3. Shmangia e falsifikimit të mesazheve

## Politikat e menaxhimit, procedurat e bizneseve dhe ligjet publike

---

- Organizatat ne USA shpenzojne 10 % te buxhetit te tyre per siguri ne harduer, softuer dhe sherbime
- Kerkohen politika menaxhuese efektive



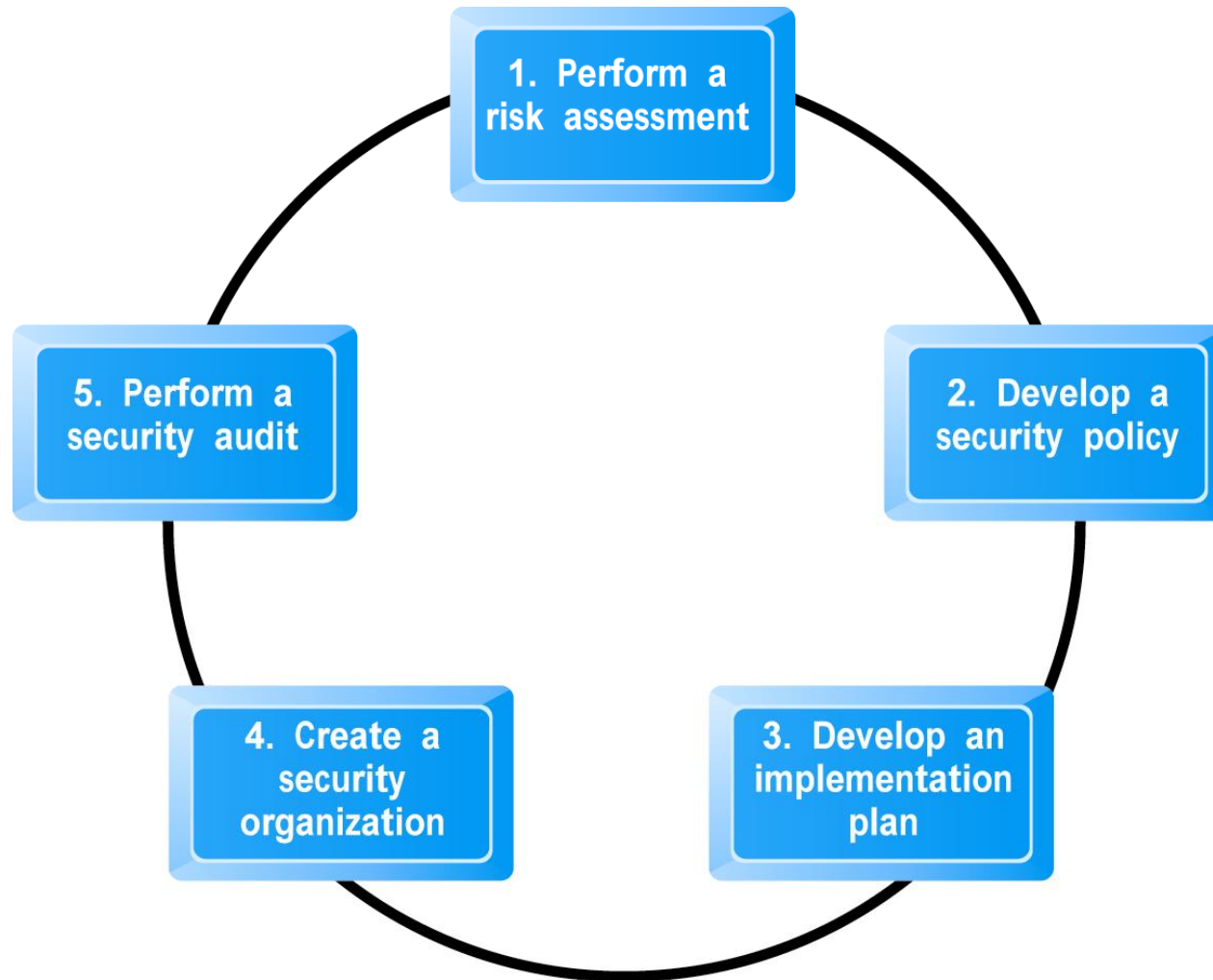
# Politikat e menaxhimit te sigurise

---

- Vleresimi i rrezikut
- Politikat e sigurise
- Plani i implementimit
  - Kontrollimi i qasjeve
  - Procedurat e autentifikimit
    - Biometrike
  - Politikat e autorizimit
    - Sistemet per menaxhimin e autorizimeve
- Auditimi i sigurise

# Zhvillimi i nje plani te sigurise ne E commerce

---



# Roli i ligjeve dhe politikave publike

---

- Ligjet e reja ju jepen autoriteteve mjete dhe mekanizma per identifikimin, gjurmimin dhe ndjekjen e krimineleve kibernetik
- Politikat qeveritare per kontrollin e enkriptimit te softuereve

# Llojet e sistemeve te pagesave

---

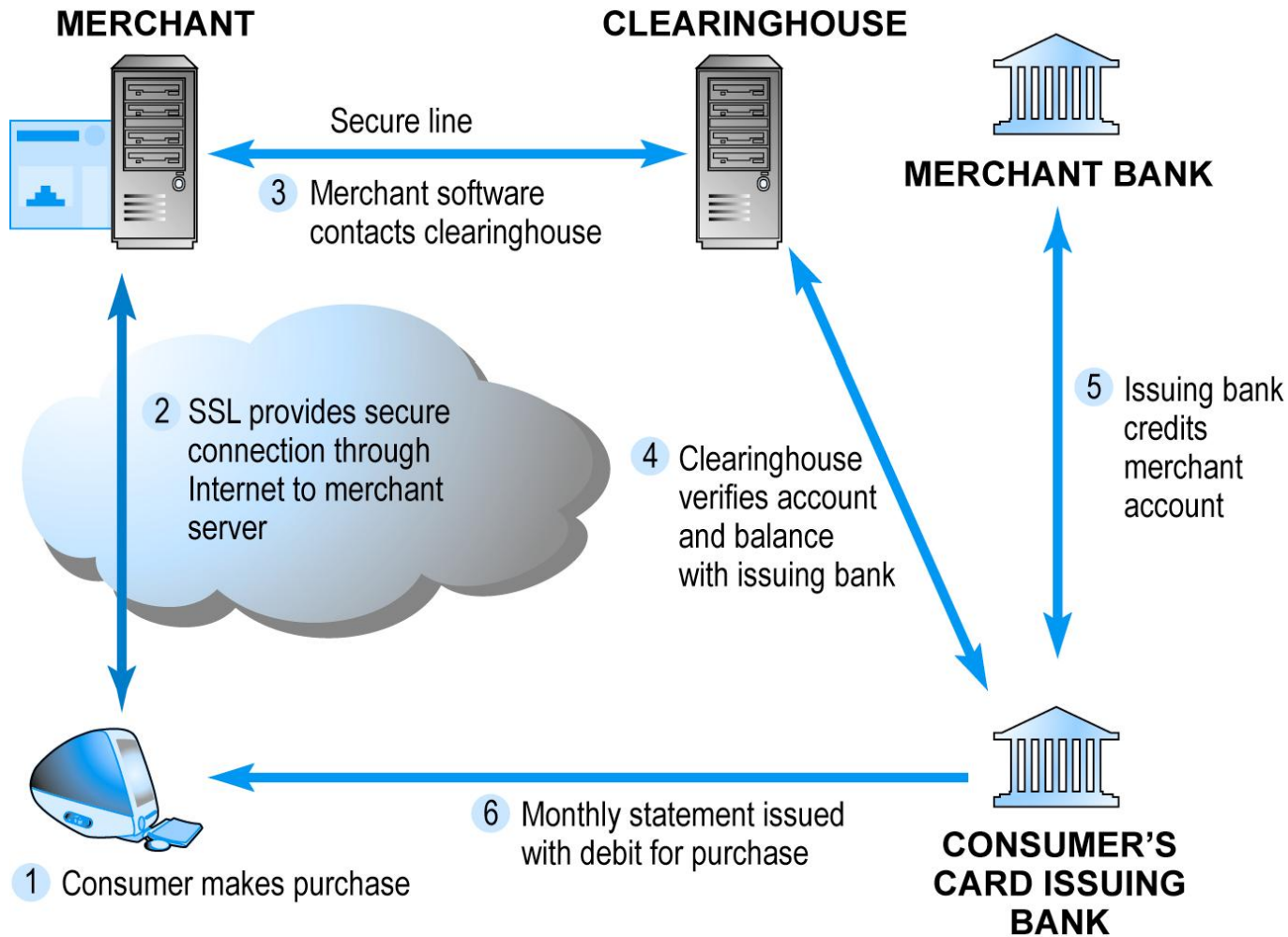
- Cash-i
- Kontrolli i transfereve
- Credit Card -at
- Balanci i akumuluar

# Sistemet e pagesave ne Ecommerce

---

- Kredit kartelat jane dominante ne pagesat online
- Sistemet tjera te pagesave ne EC:
  - Kuletat digjitale (Digital wallets)
  - Digital cash
  - Online stored value payment systems
  - Digital accumulating balance systems
  - Digital checking

# Funksionimi i nje transaksioni online permes kredit karteles



# Kufizimet e sistemeve te pagesave online

---

- Siguria:
  - As shitesi e as konsumatori nuk mund te jene plotesisht te autentifikuar
- Kostoja:
- Barazia sociale:
  - Shume njerez nuk kane qasje ne kredit karta

# Kercenimet e servereve

---

- Sa me kompleks qe eshte ueb serveri, aq me i madh eshte probabiliteti qe te kete gabime ne kodin ekzistues – vrima te sigurise nga ku hakeret mund te qasen.
- Ueb serveret ekzekutohen ne nivele te ndryshme te privilegjeve:
  - Nivelet me te larta ofrojne qasje me te madhe dhe me fleksibile per perdoruesit Ueb (nga browser-i)
  - Nivelet me te uleta ofrojne nje mbrojtje logjike rreth programit qe ekzekutohet



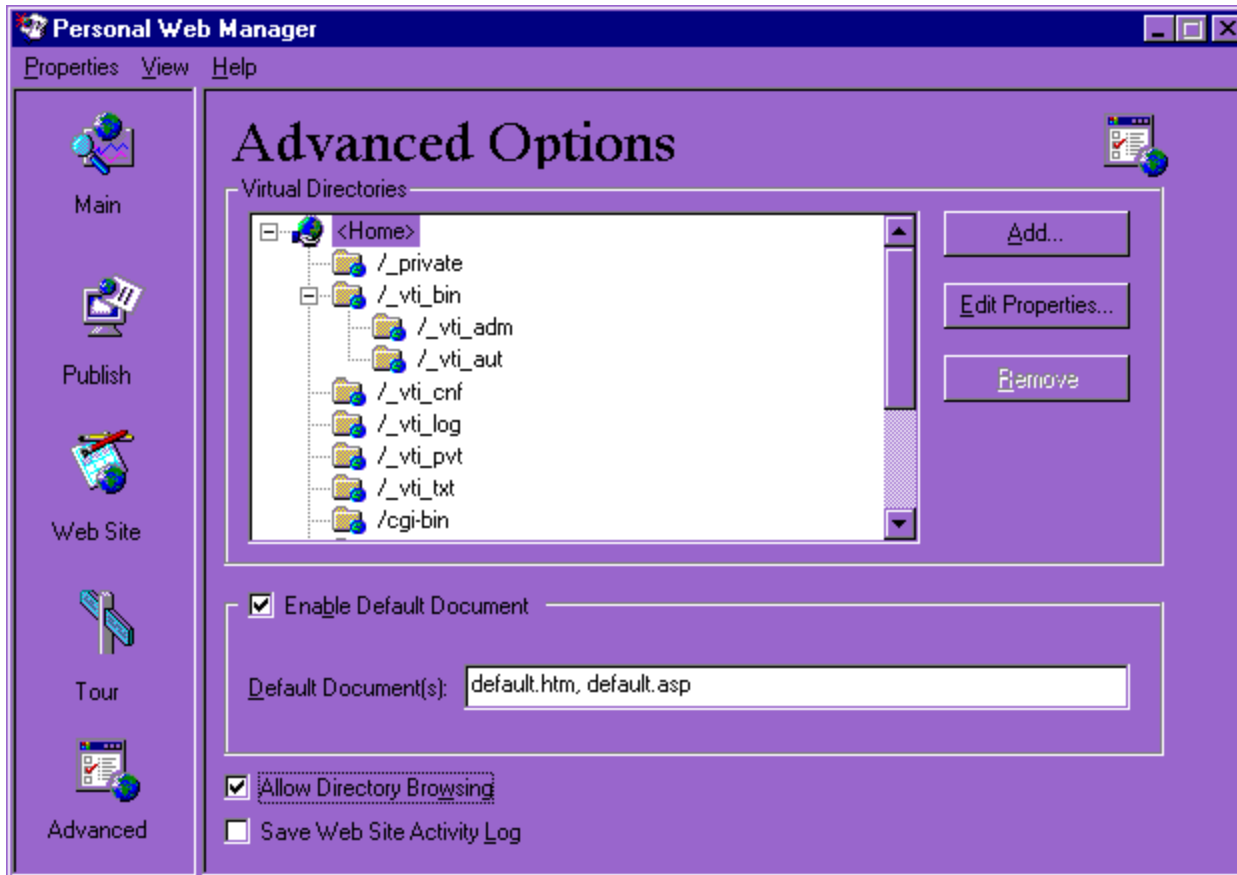
# Kercenimet e servereve

---

- Shkeljet e sigurise ndodhin kur permbajtjet e emrave te foldereve ne servere zbulohen (demaskohen) ne Ueb browser.
- Administratoret e Ueb sajtit duhet te ndalin vecorite qe shfaqin detaje te cilat mund te perdoren nga hakeret
- “Cookies” qe kerkohen nga Ueb serveri, qe permbajne UserID dhe passwordin ne kompjuterin e klientit, nuk duhet te transmetohen asnjehere si te pa mbrojtura

# Kercenimet e servereve


















---



# Shfaqja e emrave te foldereve

---

directory names

Name	Last modified	Size	Description
 <u>Parent Directory</u>	27-Feb-1999 10:52	-	
 <u>EC-Ch01.htm</u>	13-Feb-1999 15:48	2k	
 <u>EC-Ch02.htm</u>	14-Mar-1999 12:27	9k	
 <u>EC-Ch03.htm</u>	20-Apr-1999 14:38	18k	
 <u>EC-Ch04.htm</u>	03-May-1999 16:17	18k	
 <u>EC-Ch05.htm</u>	14-May-1999 09:26	7k	
 <u>EC-Ch06.htm</u>	14-May-1999 09:26	5k	
 <u>EC-Ch07.htm</u>	13-Feb-1999 15:56	2k	
 <u>EC-Ch08.htm</u>	13-Feb-1999 15:56	2k	
 <u>EC-Ch09.htm</u>	13-Feb-1999 15:59	2k	
 <u>EC-Ch0A.htm</u>	13-Feb-1999 16:01	2k	
 <u>EC-Ch10.htm</u>	13-Feb-1999 15:59	2k	
 <u>EC-Ch11.htm</u>	13-Feb-1999 15:59	2k	
 <u>EC-Ch12.htm</u>	13-Feb-1999 15:59	2k	
 <u>EC-Ch13.htm</u>	13-Feb-1999 16:01	2k	
 <u>EC-Ch14.htm</u>	13-Feb-1999 16:01	2k	
 <u>start.html</u>	15-May-1999 14:30	3k	

**FIGURE 5-9** *Displaying folder names with a Web browser*

## Kercenimet e servereve

---

- Nje nga fajllat me senzitiv ne Ueb server eshte fajlli qe permban emrin dhe fjalekalimin
- Administratoret e Ueb servereve jane pergjegjes qe ky fajll, dhe fajlla tjerë senzitiv, te jenë të sigurtë

Faleminderit!