Universiteti AAB

Lenda: Teknologjia elektronike Komerciale

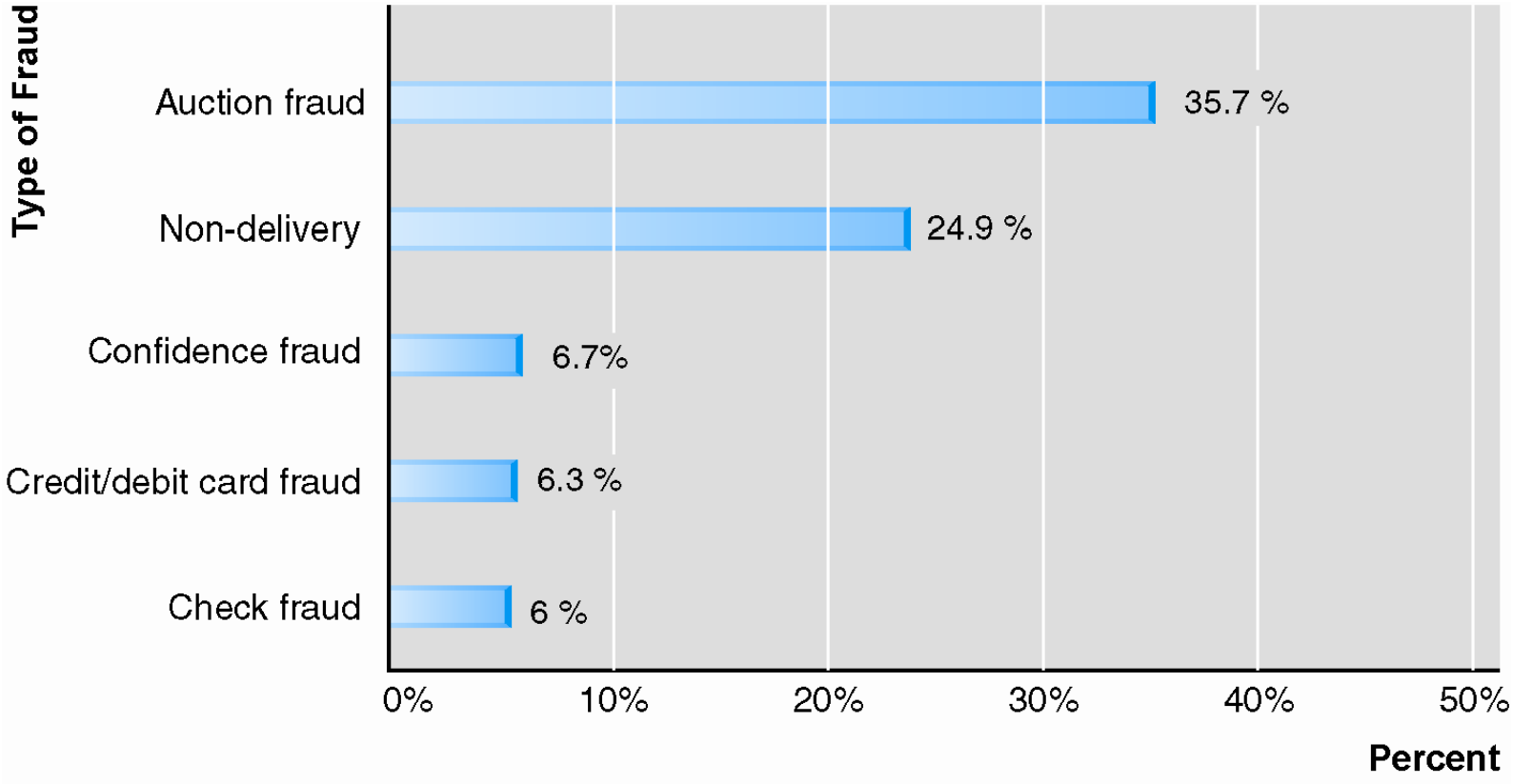
Ligjerata 5

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

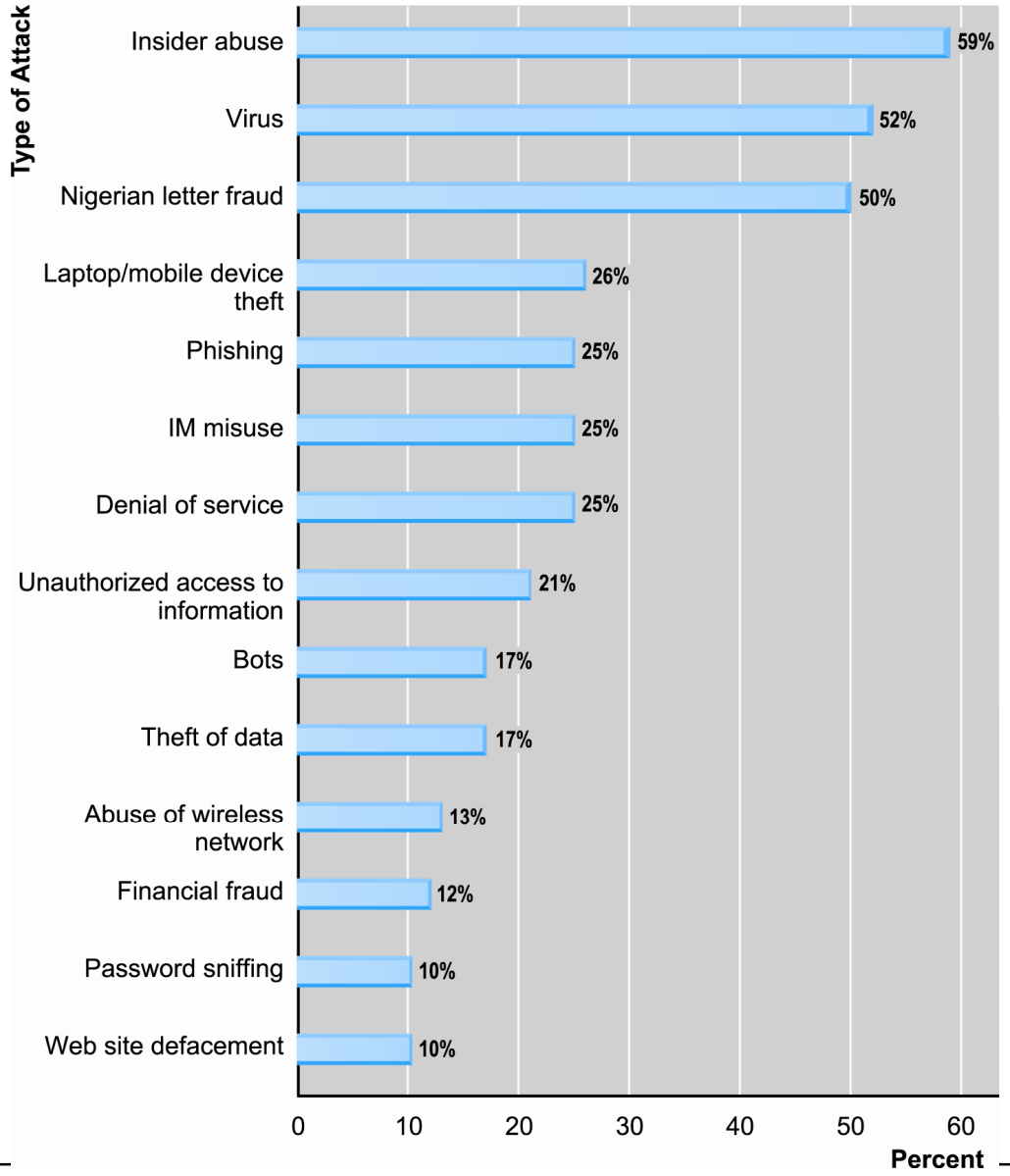
Konceptet e pergjithshme te sigurise ne E commerce?

- 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

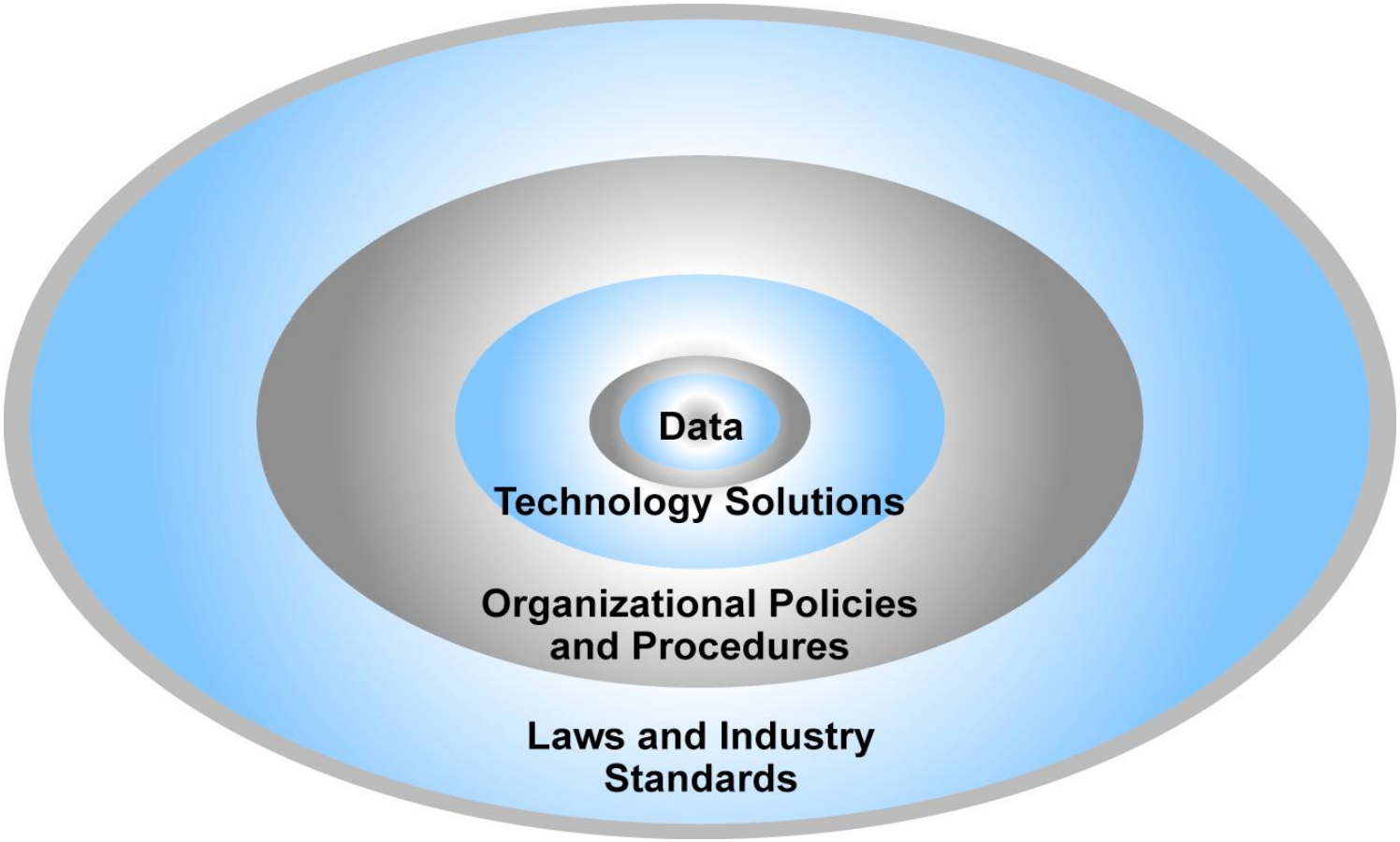
Kategorite e krimeve ne internet te raportuara ne IC3



Llojet e sulmeve kunder sistemeve kompjuterike



Mjedisi i sigurise ne EC



Siguria ne EC per nga perspektiva e konsumatorit dhe tregtarit

TABLE 5.2 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

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?

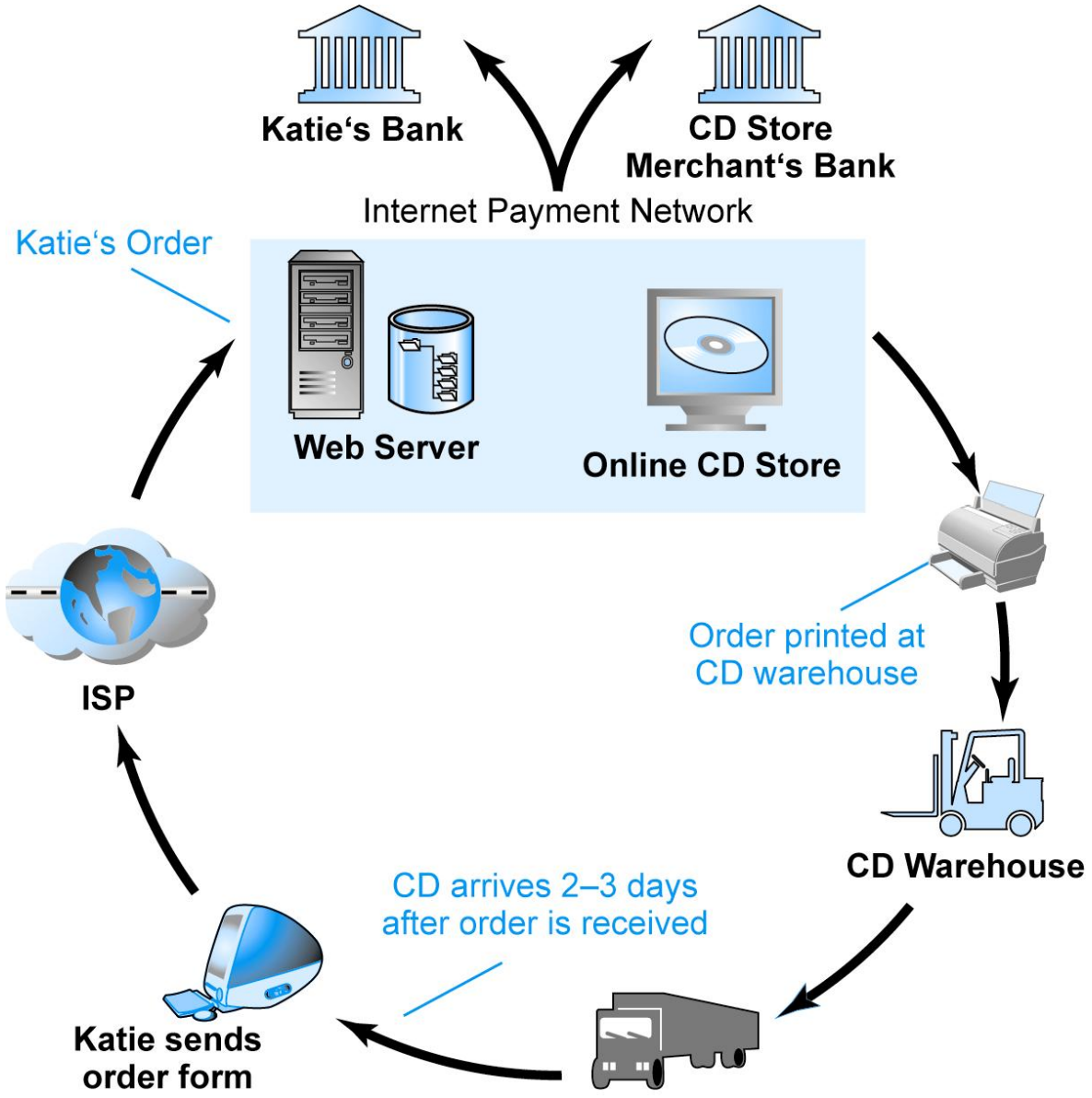
Siguria dhe vlerat tjera!

- 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 kriminelete per planifikimin e krimeve te ndryshme

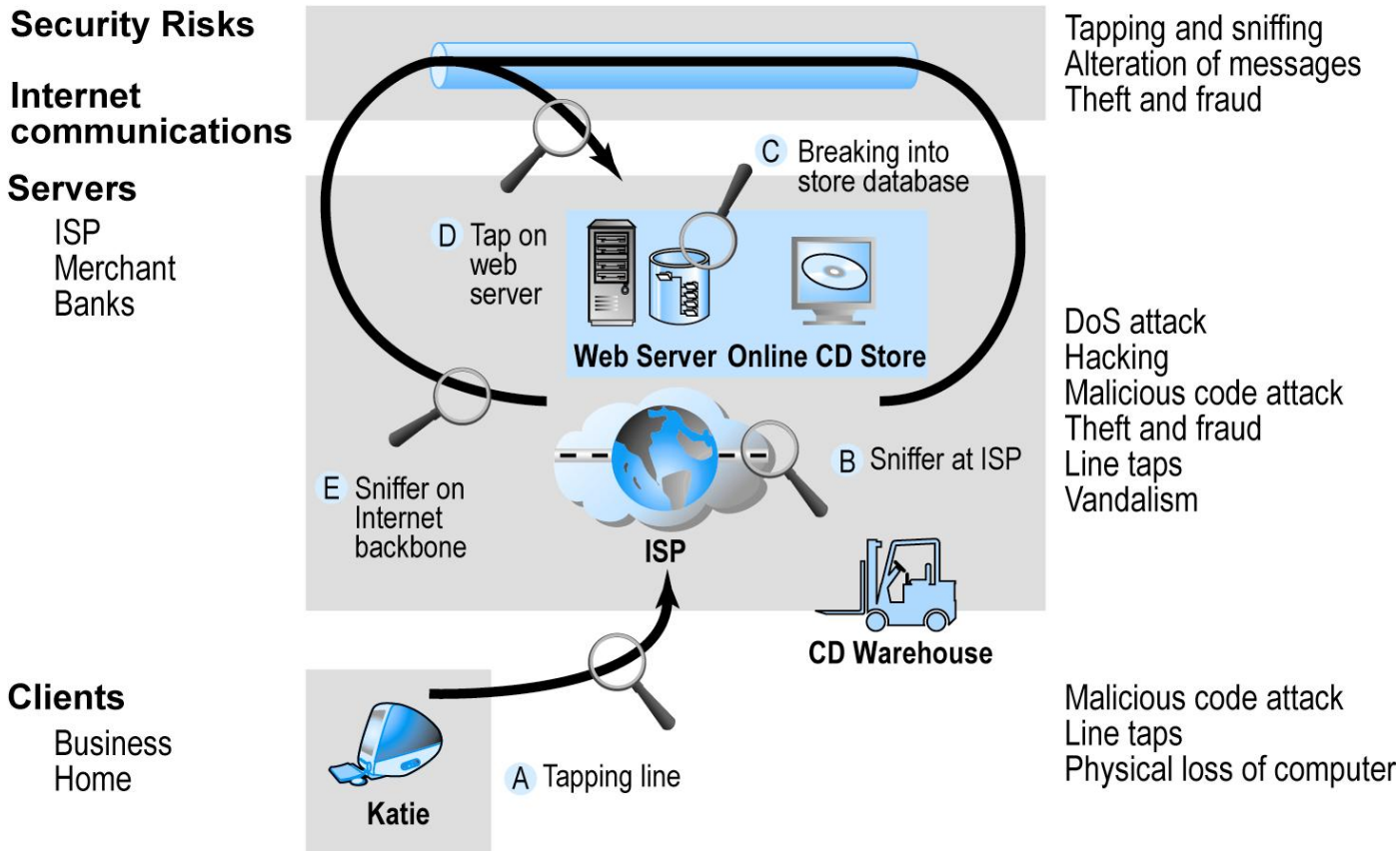
Kercenimet e sigurise ne nje mjedis EC

- Klient
- Server
- Kanalet komunikuese

Nje transaksion tipik EC



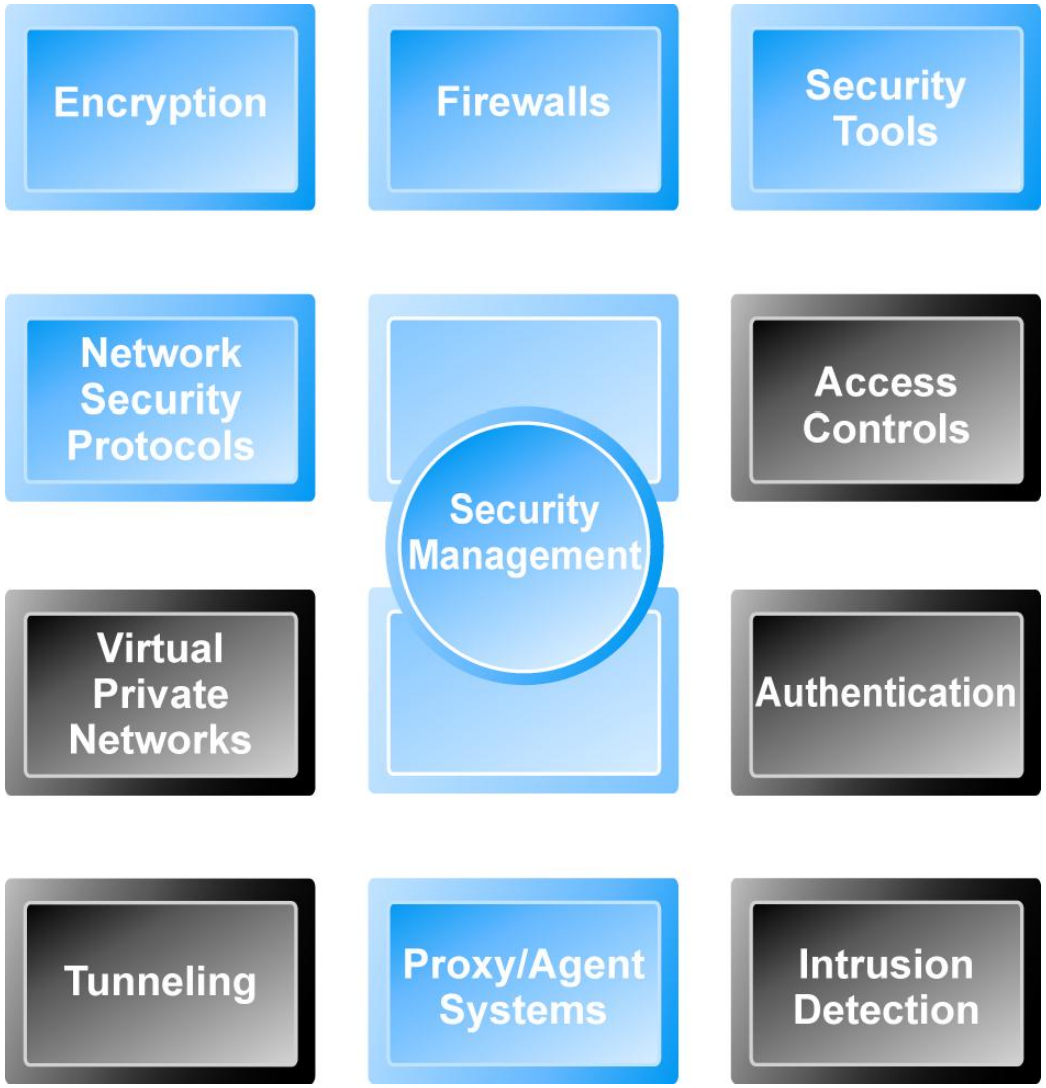
Pikat e dobeta ne nje mjedis EC



Zgjidhjet teknologjike

- Mbrojtja e komunikimeve ne Internet (encryption)
- Siguria e kanaleve kominikuese (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

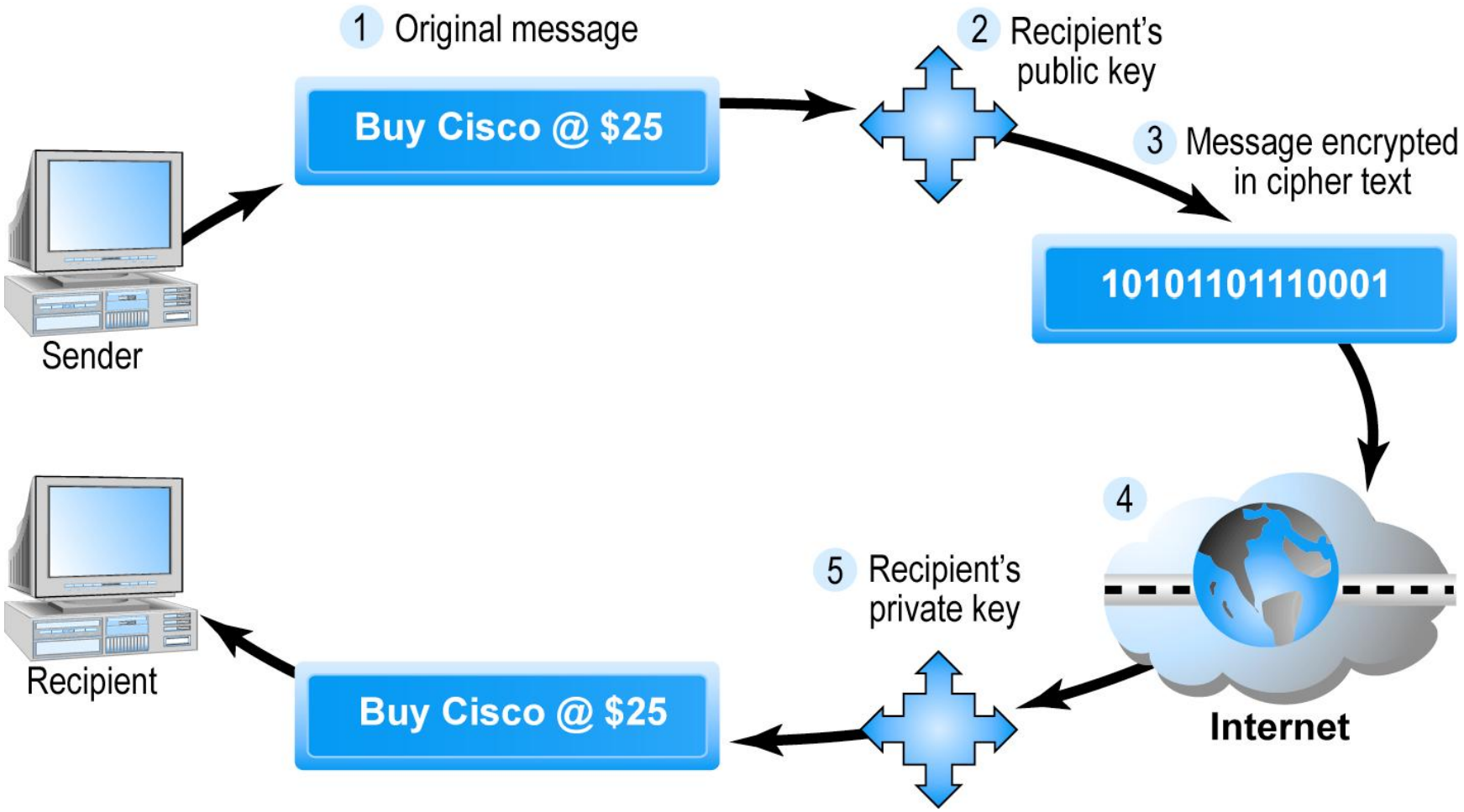
Enkriptimi me çelës simetrik

- I njohur gjithashtu si enkriptim me çelës sekret
- Derguesi dhe pranuesi e perdorin te njejtin çelës digjital per enkriptimin dhe dekriptimin e mesazhit
- Kerkohen çelësa te ndryshem per secilin transaksion
- AES (Advanced Encryption Standard)
  - Enkriptimi me i perdorur me çelës simetrik
  - Perdor çelësa per enkriptim prej 128-, 192-, dhe 256-bit
- Standardet tjera perdorin çelësa deri ne 2,048 bits

Enkriptimi me çelës publik

- Perdor dy çelësa te nderlidhur matematikisht njeri me tjetrin
  - çelësin publik
  - çelësin privat (mbahet sekret nga zoteruesi)
- Te dy çelësat perdoren per enkriptim dhe dekriptim te mesazheve
- Kur njeri çelës perdoret per enkriptim te mesazhit, i njejti nuk mund te perdoret per dekriptim te mesazhit
- Derguesi e perdor çelësin publik te pranuesit per enkriptim te mesazhit; pranuesi perdor çelësin e tij privat per dekriptim te mesazhit

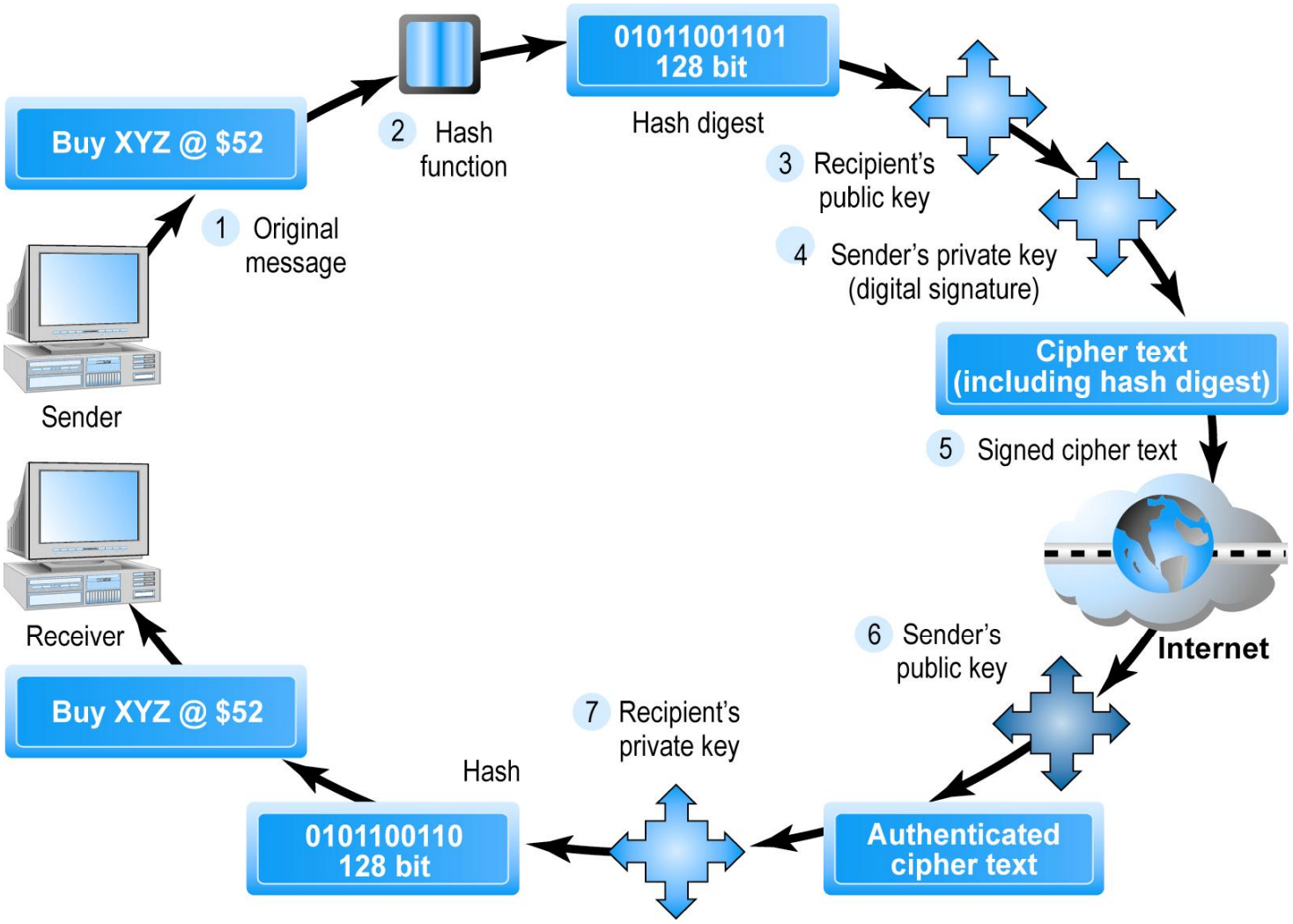
Kriptografia me çelës publik - shembull



Enkriptimi me çelës publik duke perdorur nenshkrimet digjitale dhe “Hash Digests”

- Hash funksioni:
  - Algoritem matematik qe prodhon nje numer te gjatesise fikse qe quhet mesazh ose “hash digest”
- “Hash digest” dhe mesazhi i enkriptuar me çelësin publik te pranuesit
- I tere teksti i koduar mandej enkriptohet me çelësin privat te pranuesit – duke krijuar nje nenshkrim digjital – per autenticitet.

Kriptografia me çelës publik me nenshkrim digjital

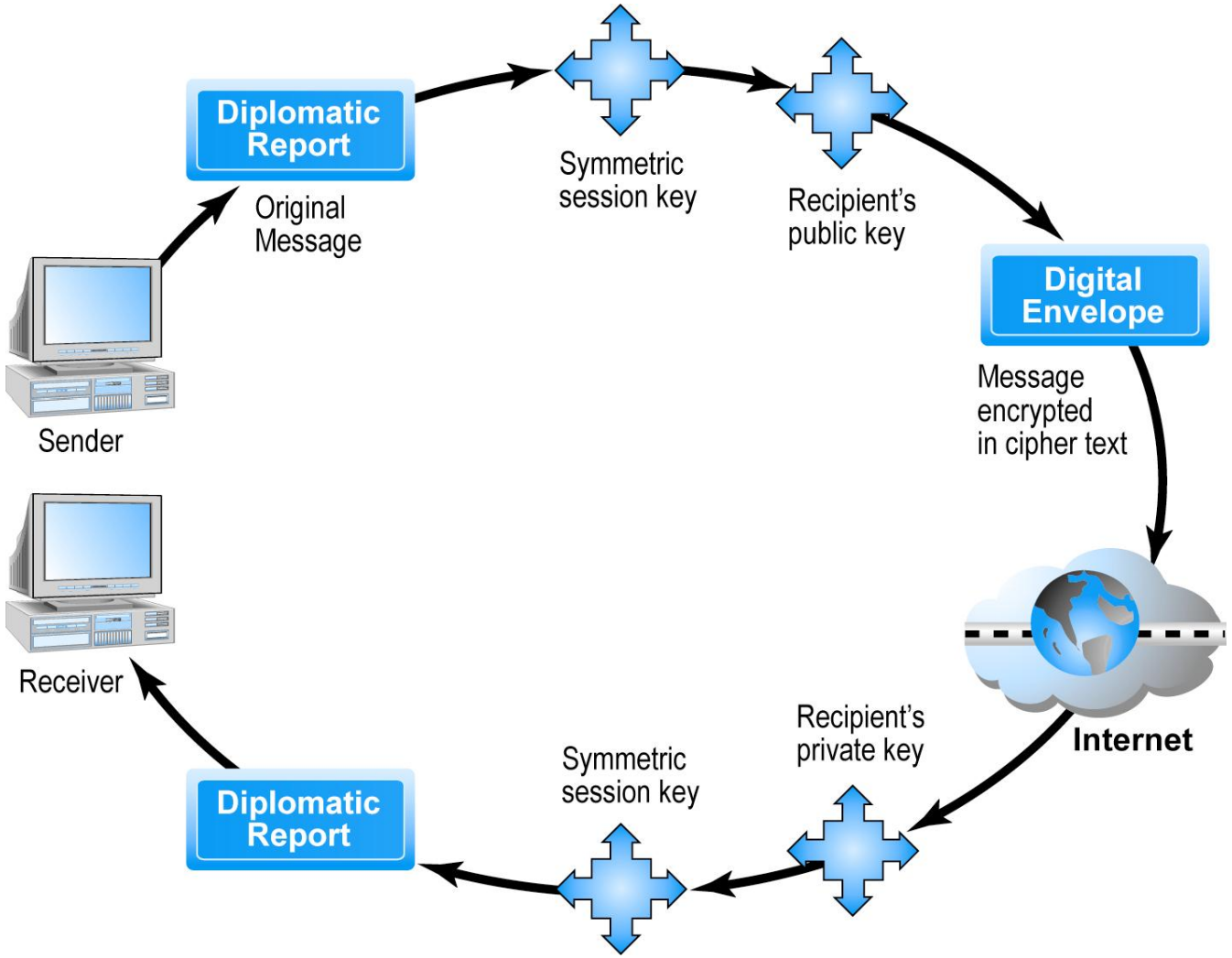


Mbeshtjellesit digjital (Digital Envelopes)

- 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

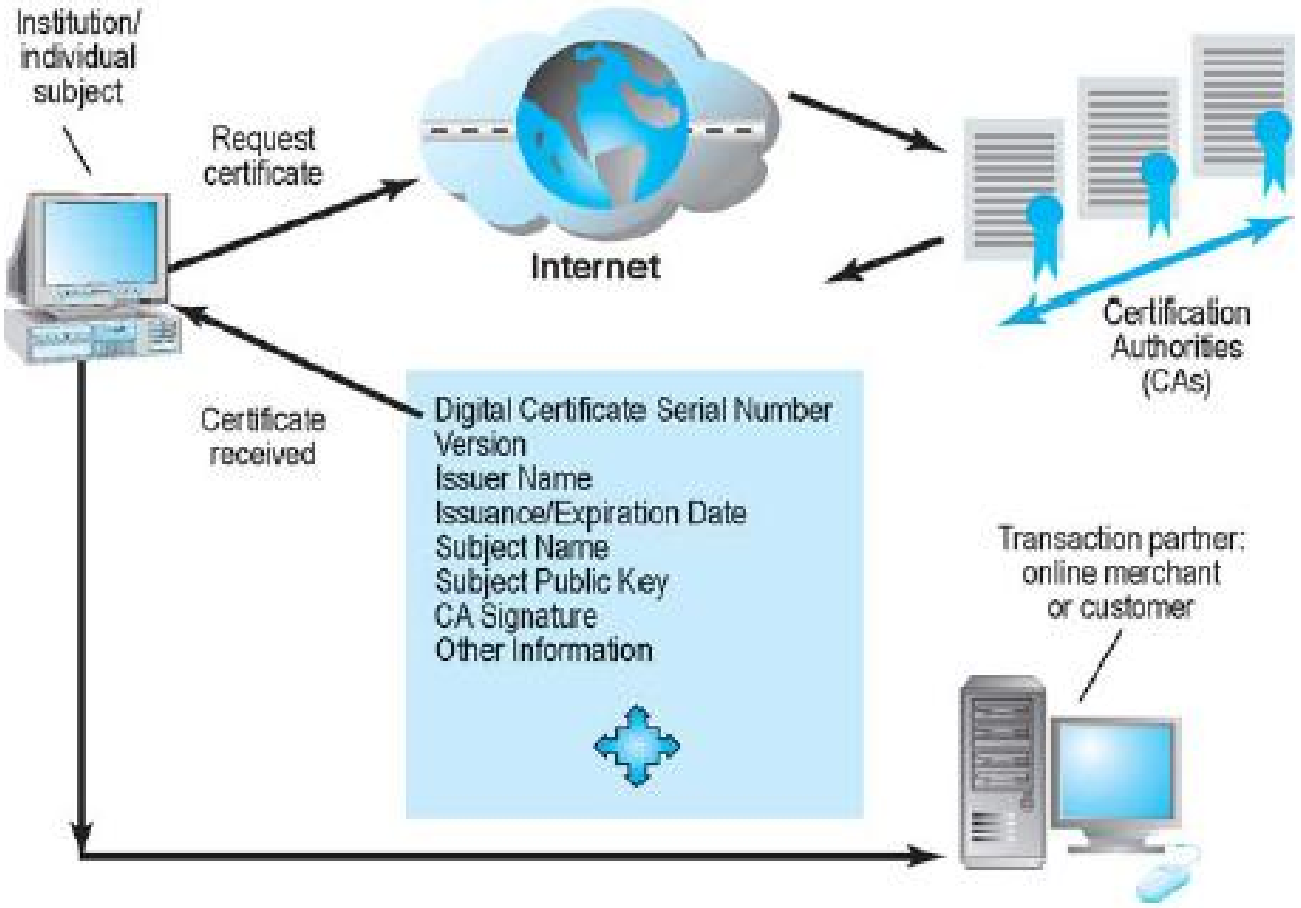
Krijimi i mbeshtjellesave digjital



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



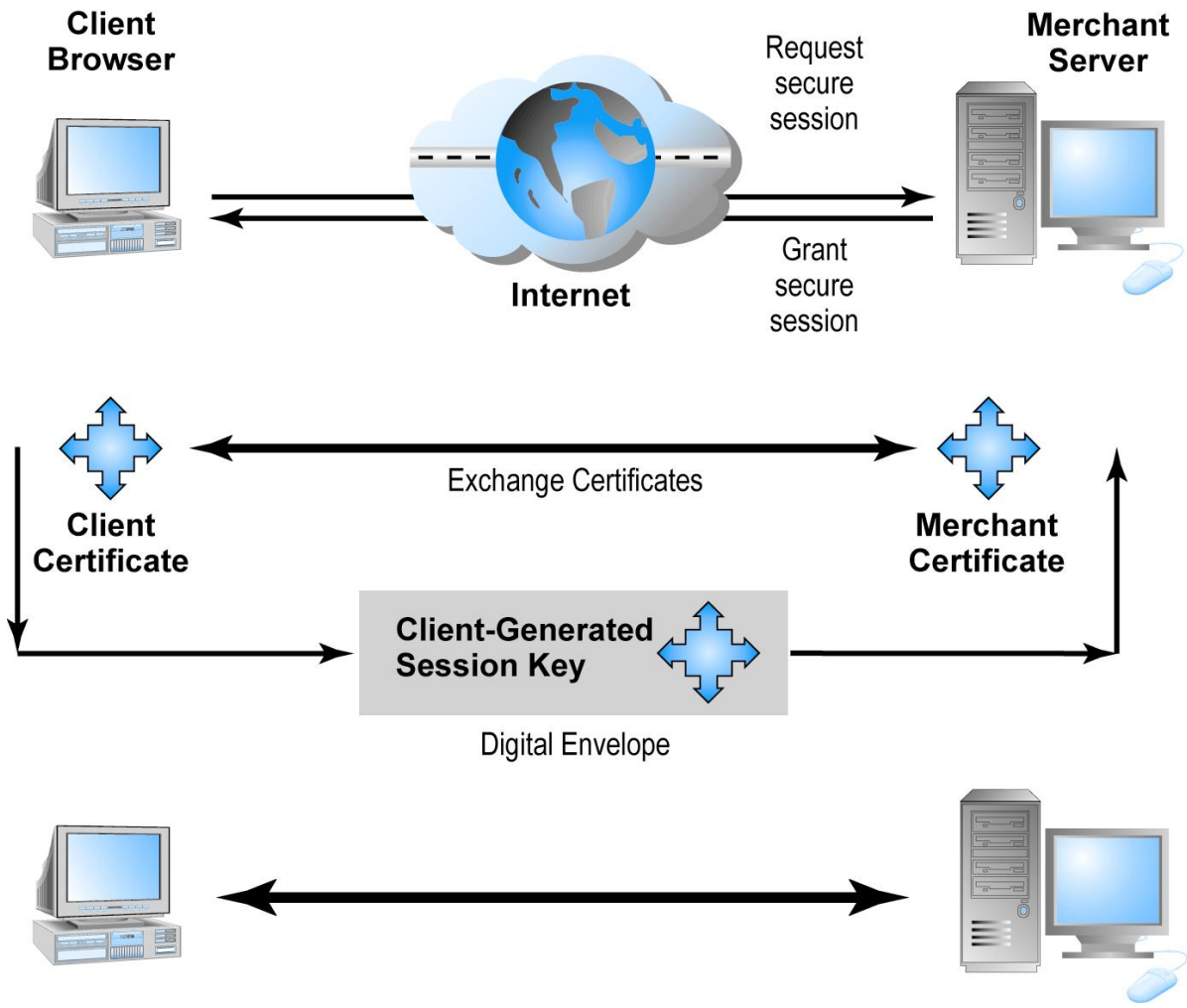
Kufizimet qe ekzistojne ne teknikat e enkriptimit

- PKI 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 dokuemtit 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)

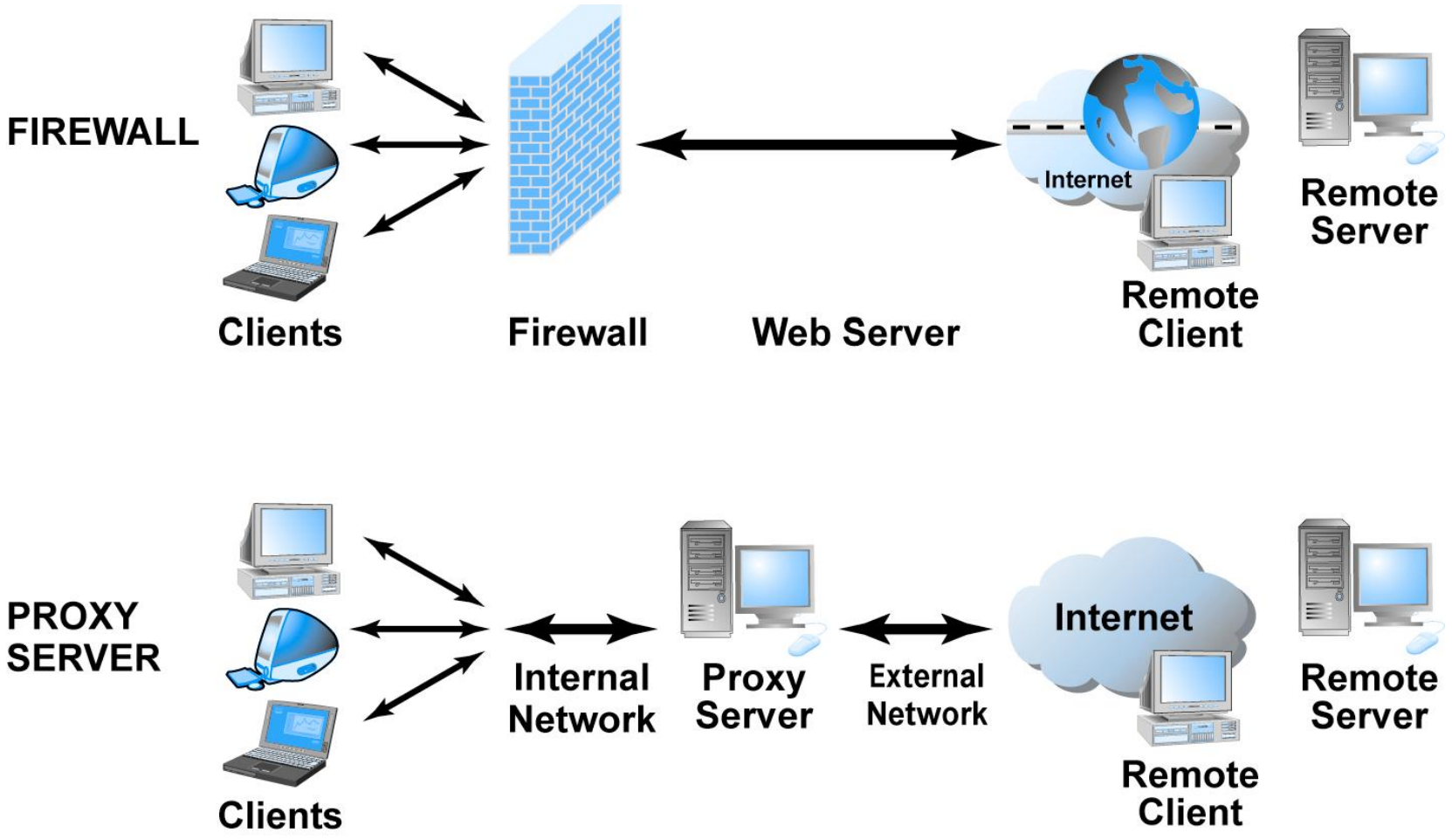
Siguria e nje sesioni duke perdorur SSL



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

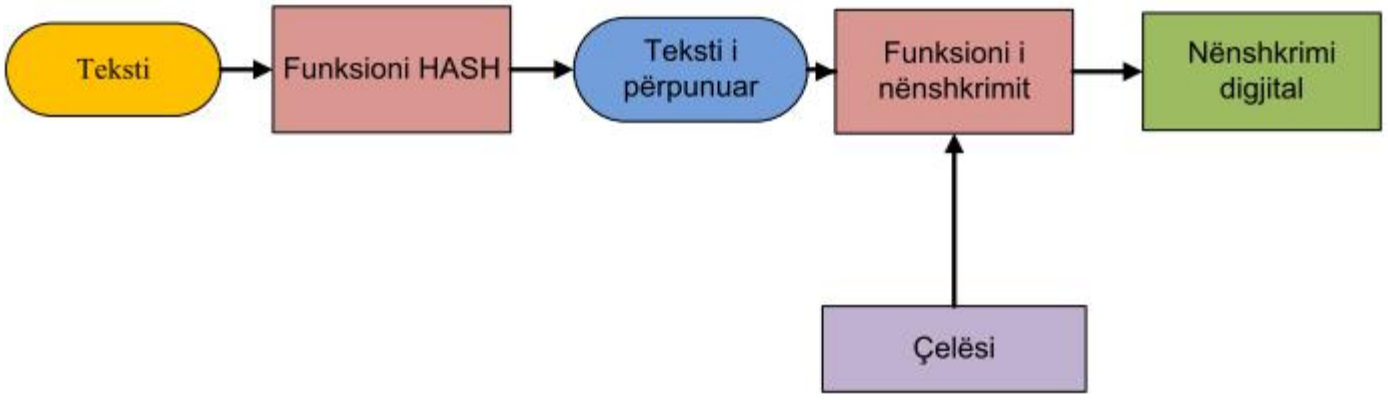
- Kontrollat ne sistemin operativ:
  - Autentifikimi dhe mekanizmat e kontrollit te qasjes
- Softueri Anti Virus:
  - Menyra me e lehte dhe me pak e kushtueshme per parandalimin e kercenimeve
  - Kerkohen perditesime ne baza ditore

Nenshkrimet digjitale

- Duke përdorur nënshkrim digjital mesazhi mund të nënshkruhet nga një pajisje që përdor çelësin privat të mesazhit për ta vërtetuar origjinalitetin e tij.
- Çdo pajisje që ka qasje deri te çelësi publik i pajisjes së nënshkruar mund ta vërtetojë nënshkrimin.
- Pajisja që e pranon mesazhin mund të sigurojë që mesazhi është i nënshkruar nga pajisja e dedikuar dhe nuk modifikohet gjatë transferimit.
- Nëse të dhënat apo nënshkrimi modifikohen ose ndryshohen, verifikimi i nënshkrimit do të dështojë.

Nenshkrimet digjitale

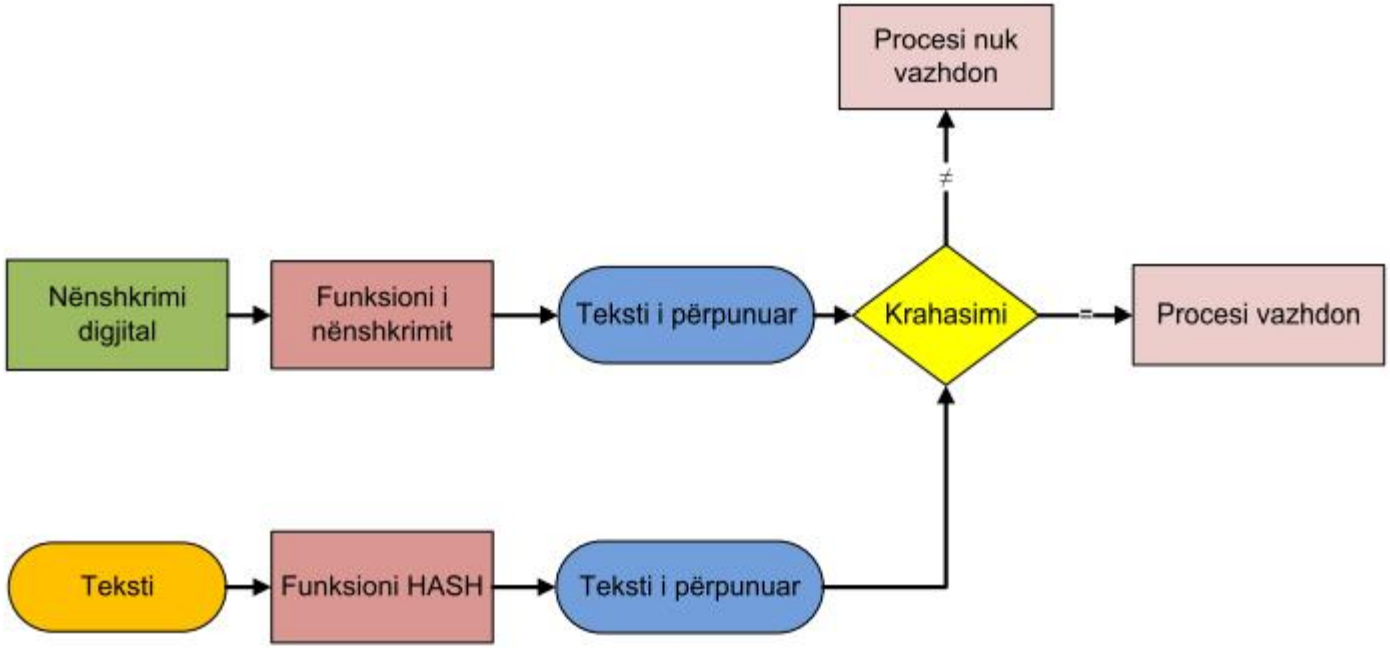
- Nënshkrimi digjital është një metodë për enkriptimin e mesazheve (siç janë dokumentet, kontratat, shpalljet) që do të transferohen, duke e adoptuar protokollin për shkëmbim të të dhënave dhe algoritmin për enkriptim të të dhënave.
- Në këtë proces fitohet një abstrakt i cili duket si nënshkrim ose 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 mesazhit që është nga dërguesi, nga ana e pranuesit.

Verifikimi i nënshkrimit digjital



Verifikimi i nënshkrimit digjital

- Për shembull, sistemi kompjuterik mund të menaxhojë me kohën dhe datën duke shtuar automatikisht vula kohore te fajlli. Skema e nënshkrimit digjital është e sigurt sepse këto skema bazohen në teknologjinë e enkriptimit që në mënyrë të sigurt mbështetet në algoritme konkrete.
- Algoritmi më i zakonshëm për nënshkrim digjital duhet të sigurojë që nënshkrimi është anti-refuzues, anti-përsëritës dhe mesazhi është e pamundur të ndryshojë.
- Nënshkrimi duhet tu rezistojë të gjitha llojeve të mundshme të sulmeve [5].

Politikat e menaxhimit, procedurat e bizneseve dhe ligjet publike

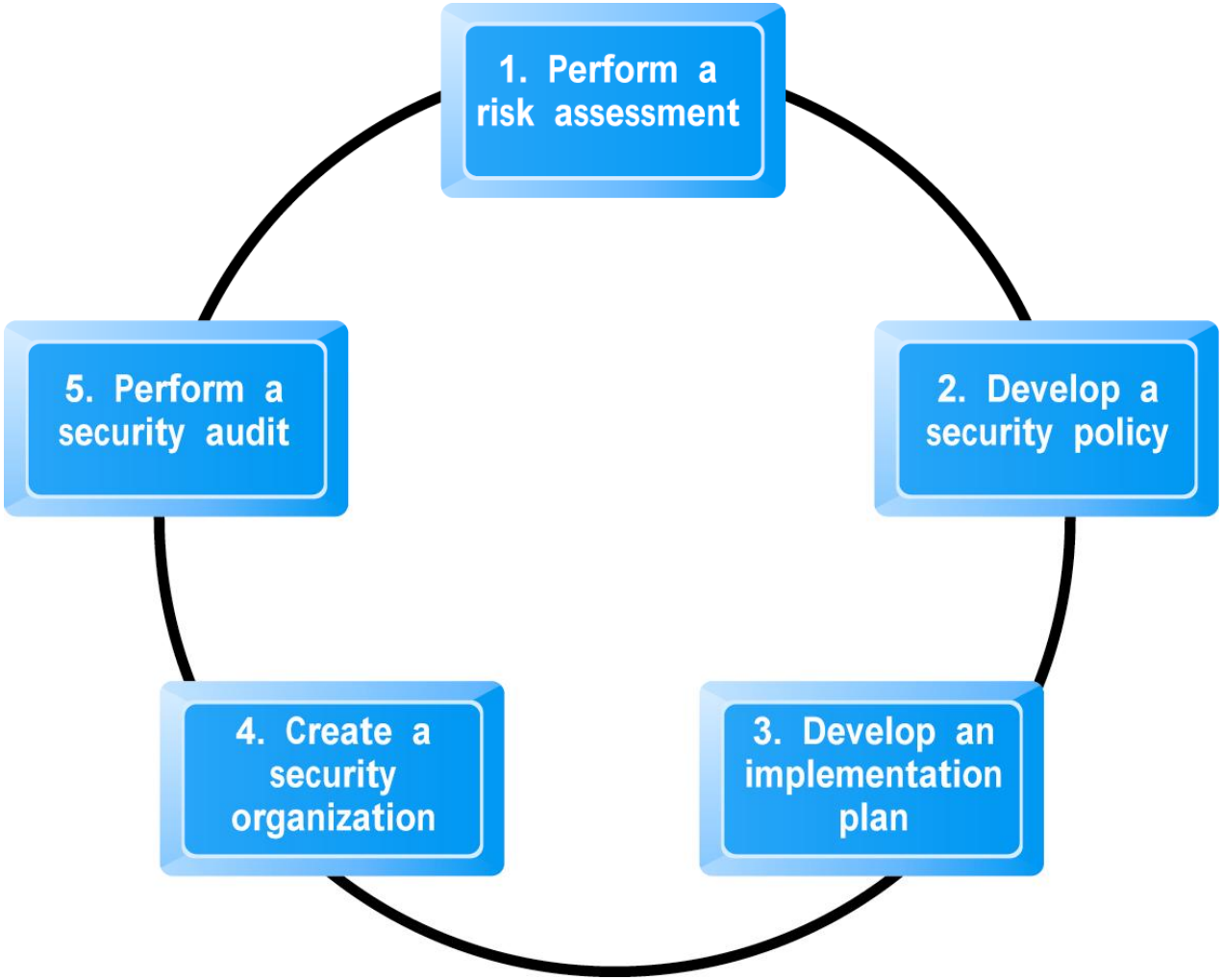
- Organizatat ne USA shpenzojne 10 % te buxhetit te tyre per siguri ne harduer, softuer dhe sherbime

- Kerkohen politika menaxhuese efektive

Plani per siguri: 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 jepin autoriteteve mjete dhe mekanizma per identifikimin, gjurmimin dhe ndjekjen e krimineleve kibernetik

- Politikat qeveritare per kontrollin e enkriptimit te softuereve

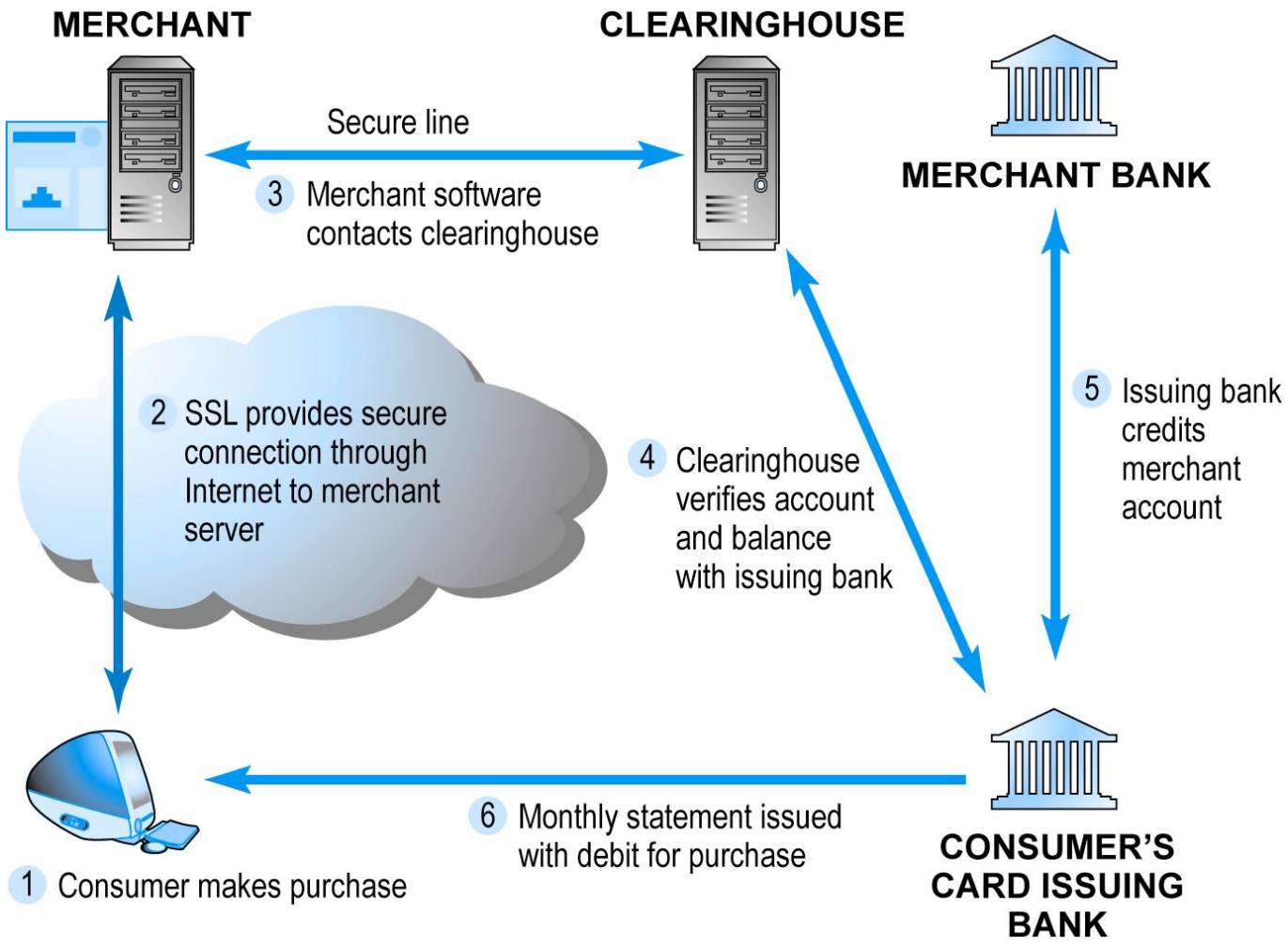
Llojet e sistemeve te pagesave

- 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

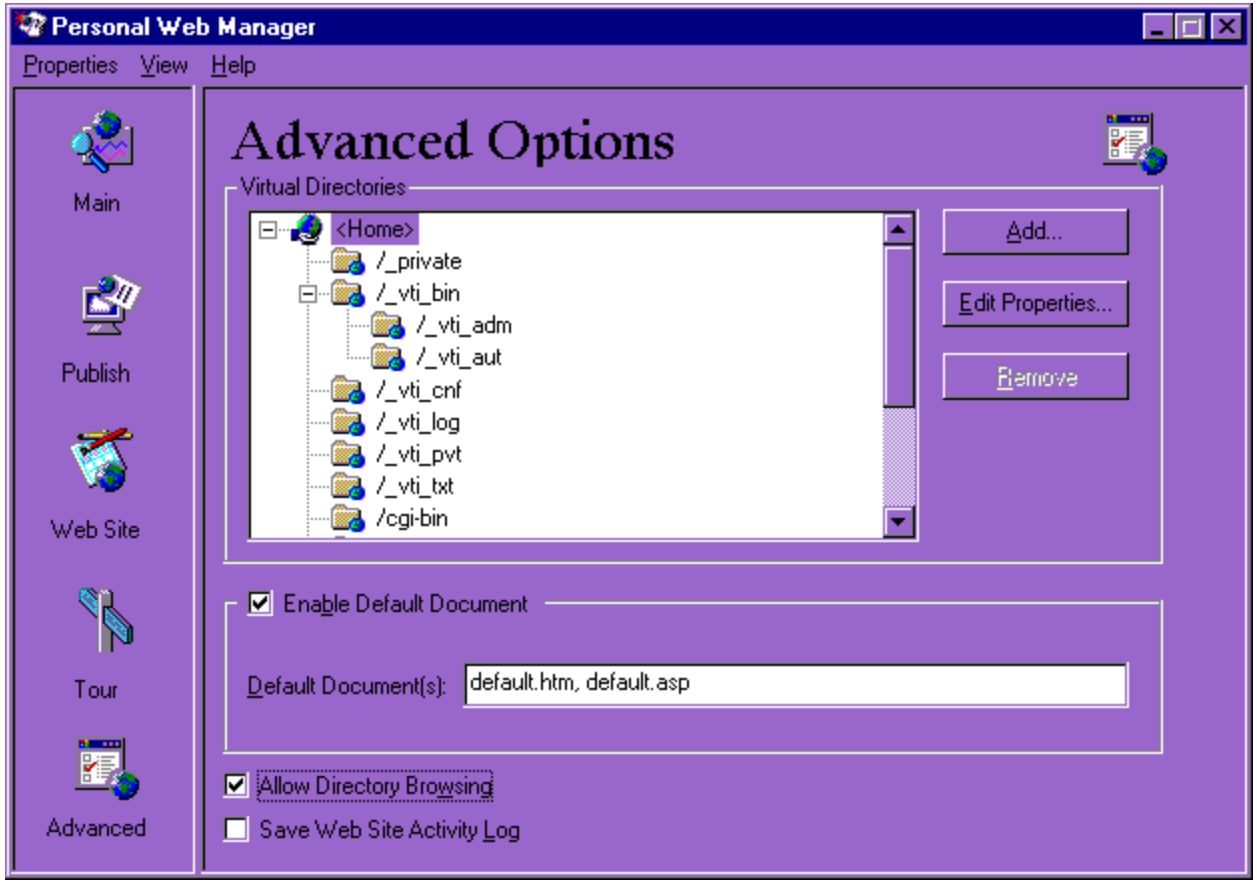
- Sa me kompleks qe eshte ueb serveri, aq me i madh eshte probabiliteti qe te kete gabime ne kodin ekzistues – vrima te sigurise nga ku hakeret mund te qasen.

- 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 kleintit, nuk duhet te transmetohen asnjehere si te pa mbrojtura

Kercenimet e servereve



Shfaqja e emrave te foldereve

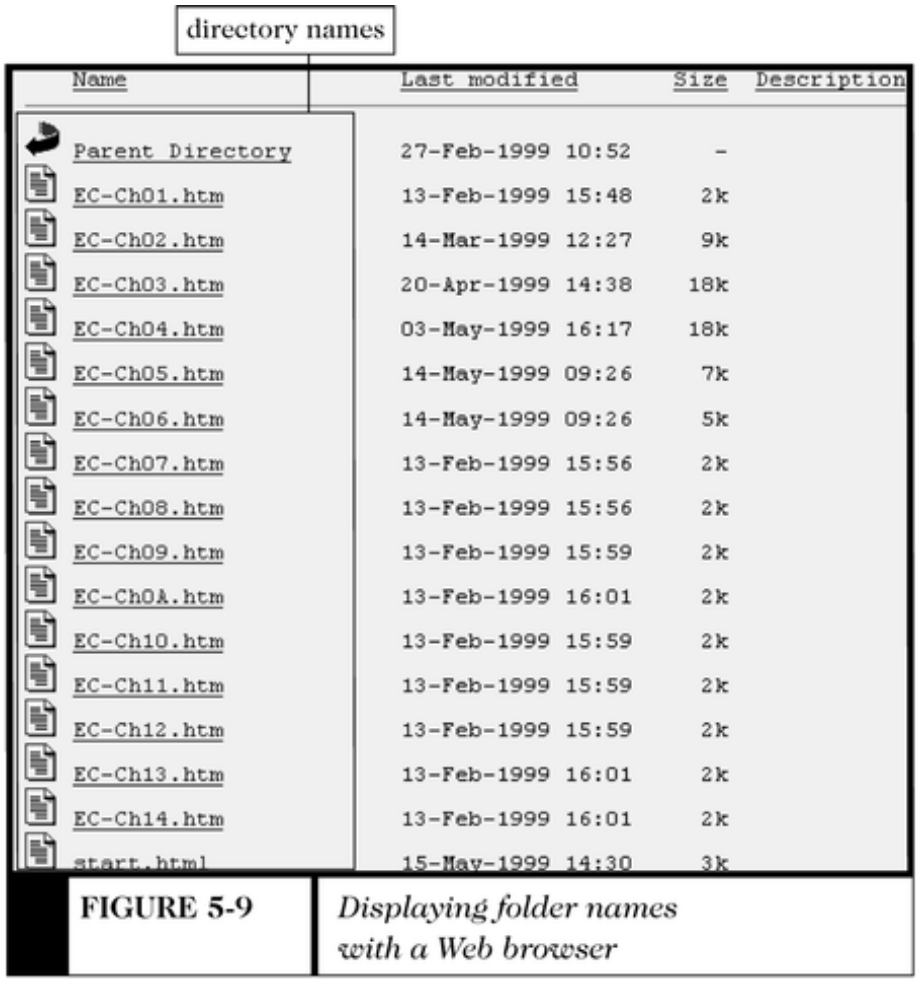


FIGURE 5-9 *Displaying folder names with a Web browser*

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!