მომავალი შენ გეკუთვნის!!!

Next-IT Academy
ნექსთ აიტი აკადემია

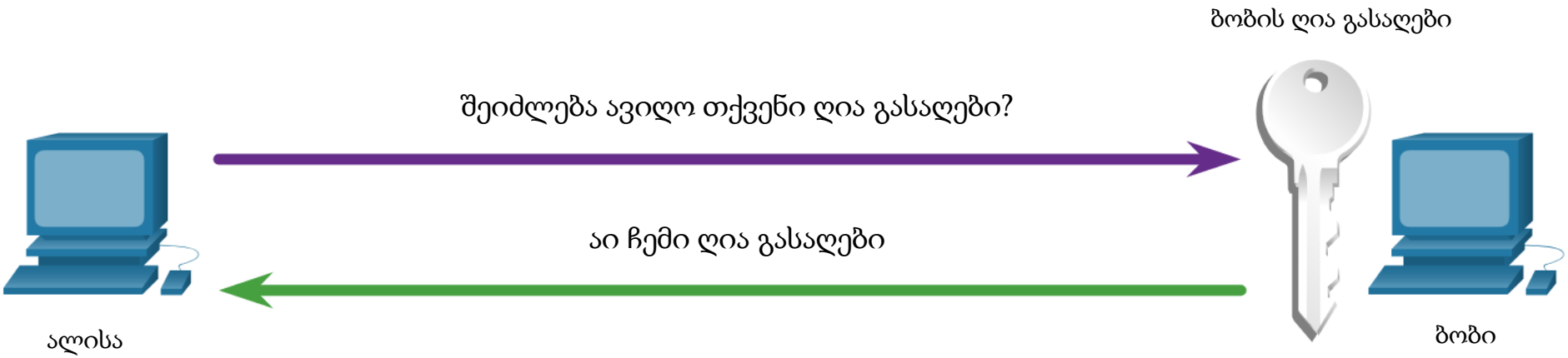
კრიპტოგრაფია ღია გასაღებით

ასიმეტრიული გასაღების მახასიათებლები

პროტოკოლები, რომლებიც იყენებენ ასიმეტრიული გასაღების ალგორითმებს:

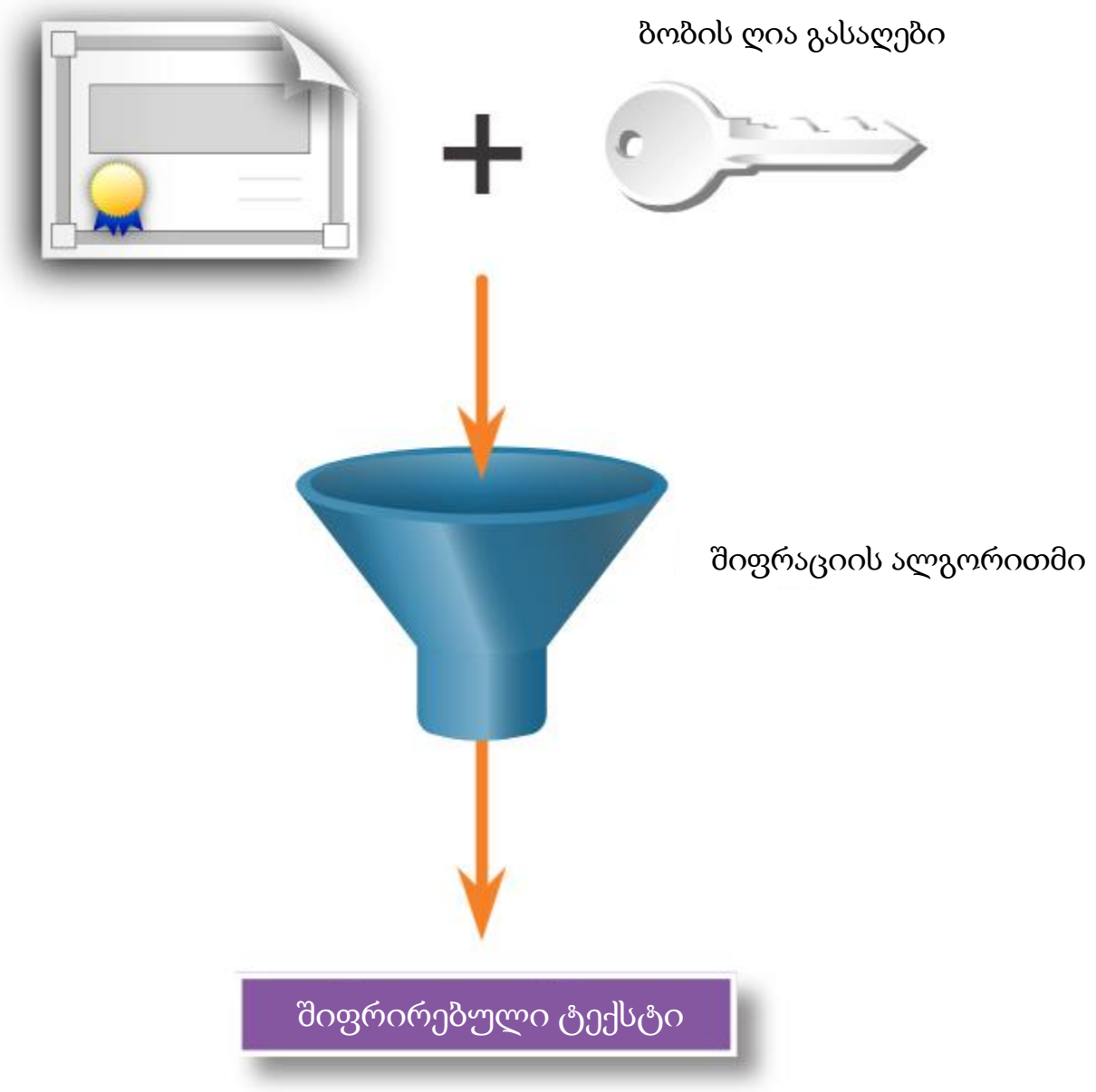
- Internet Key Exchange (IKE)
- Secure Socket Layer (SSL)
- Secure Shell (SSH)
- Pretty Goog Privacy (PGP)

ღია გასაღებს + დახურული გასაღები = კონფიდენციალობას
ალისა ითხოვს ბობის ღია გასაღებს

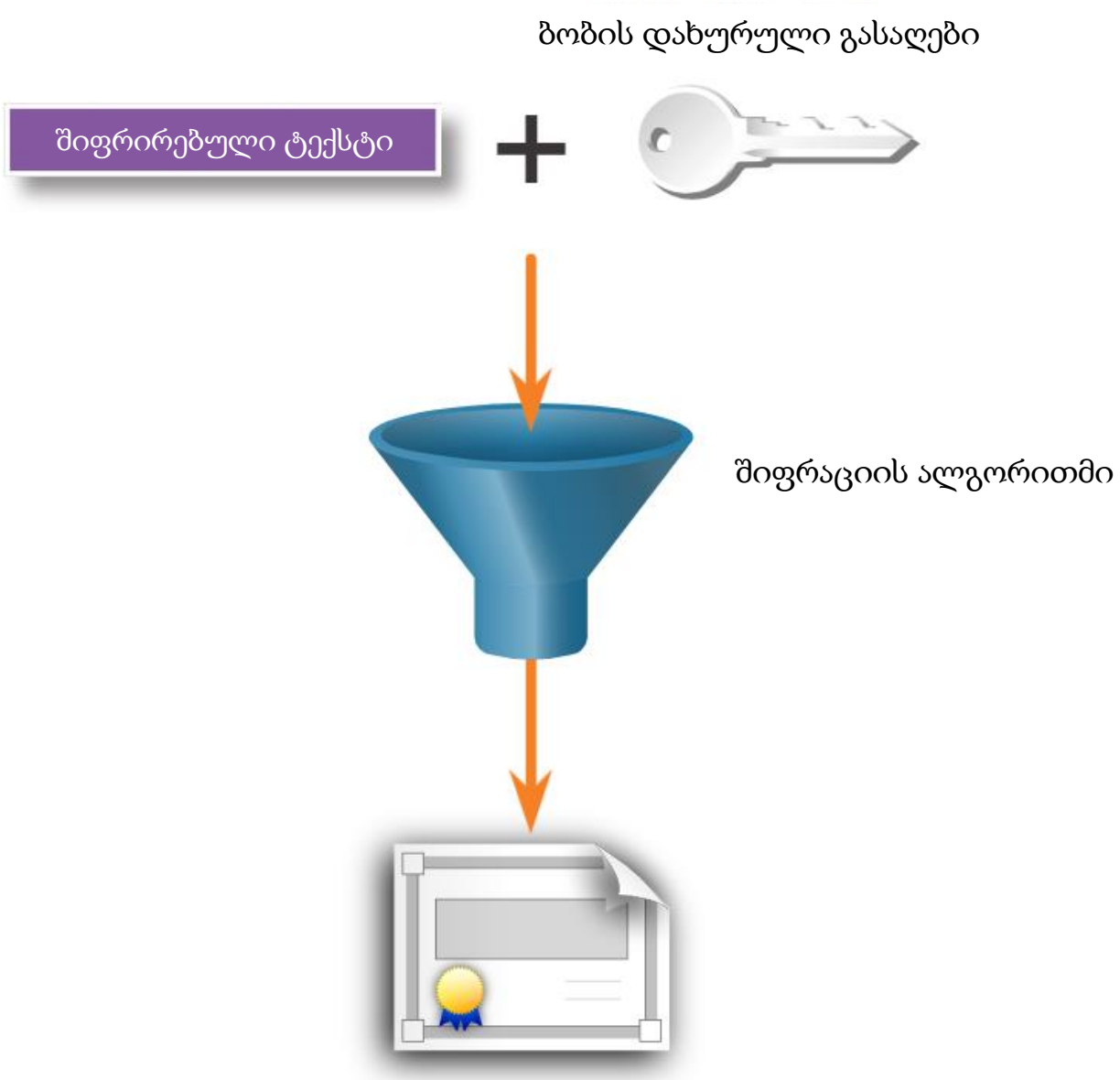


ღია გასაღები (შიფრაცია) + დახურული გასაღები (დეშიფრაცია) = კონფიდენციალობა

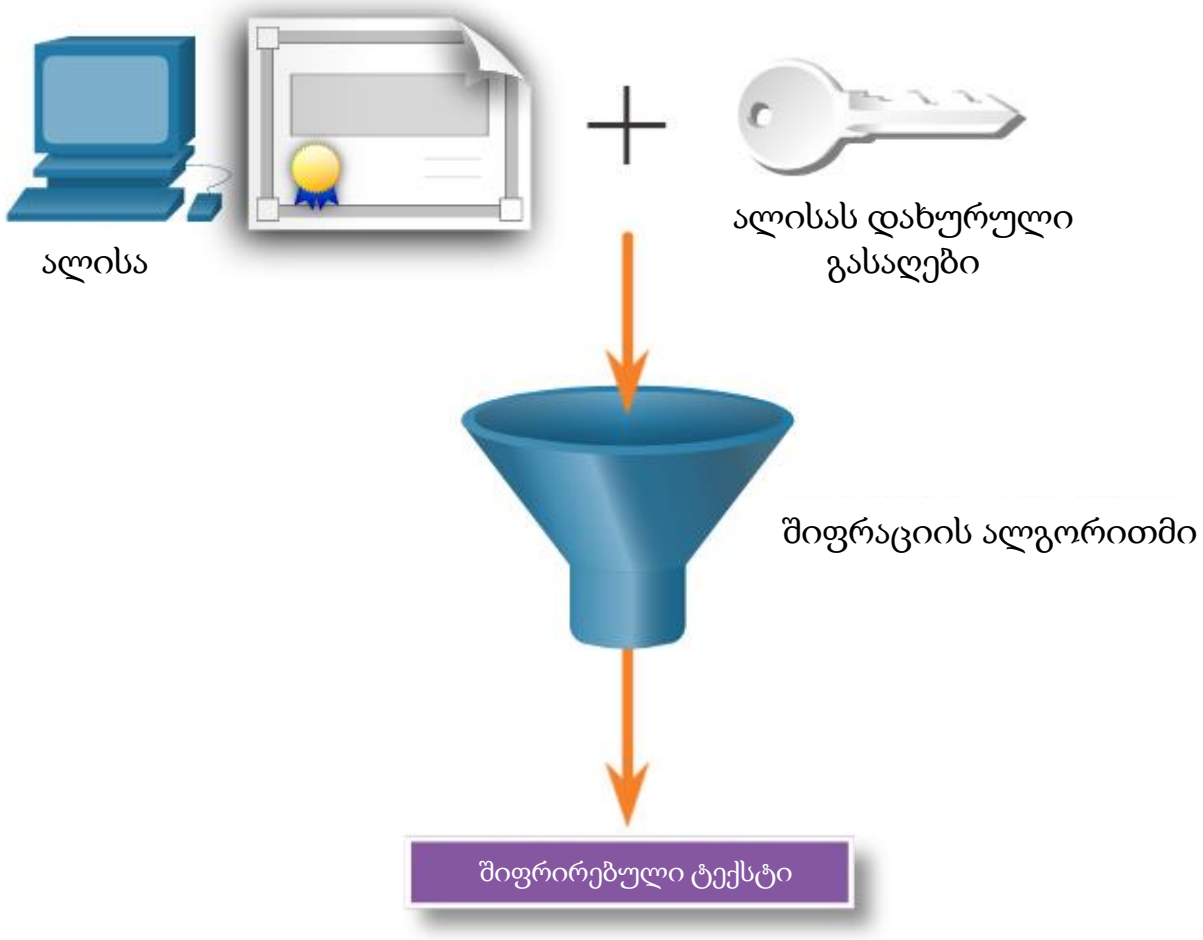
ღია გასაღებს + დახურული გასაღები = კონფიდენციალურობას
ალისა შიფრავს შეტყობინებას ბობის ღია გასაღების გამოყენებით



ღია გასაღებს + დახურული გასაღები = კონფიდენციალურობას - ბობი ახდენს შეტყობინების დეშიფრაციას თავისი დახურული გასაღების გამოყენებით



დახურულ გასაღებს + ღია გასაღები = აუთენტიკაციას - ალისა შიფრავს შეტყობინებას თავისი დახურული გასაღებით

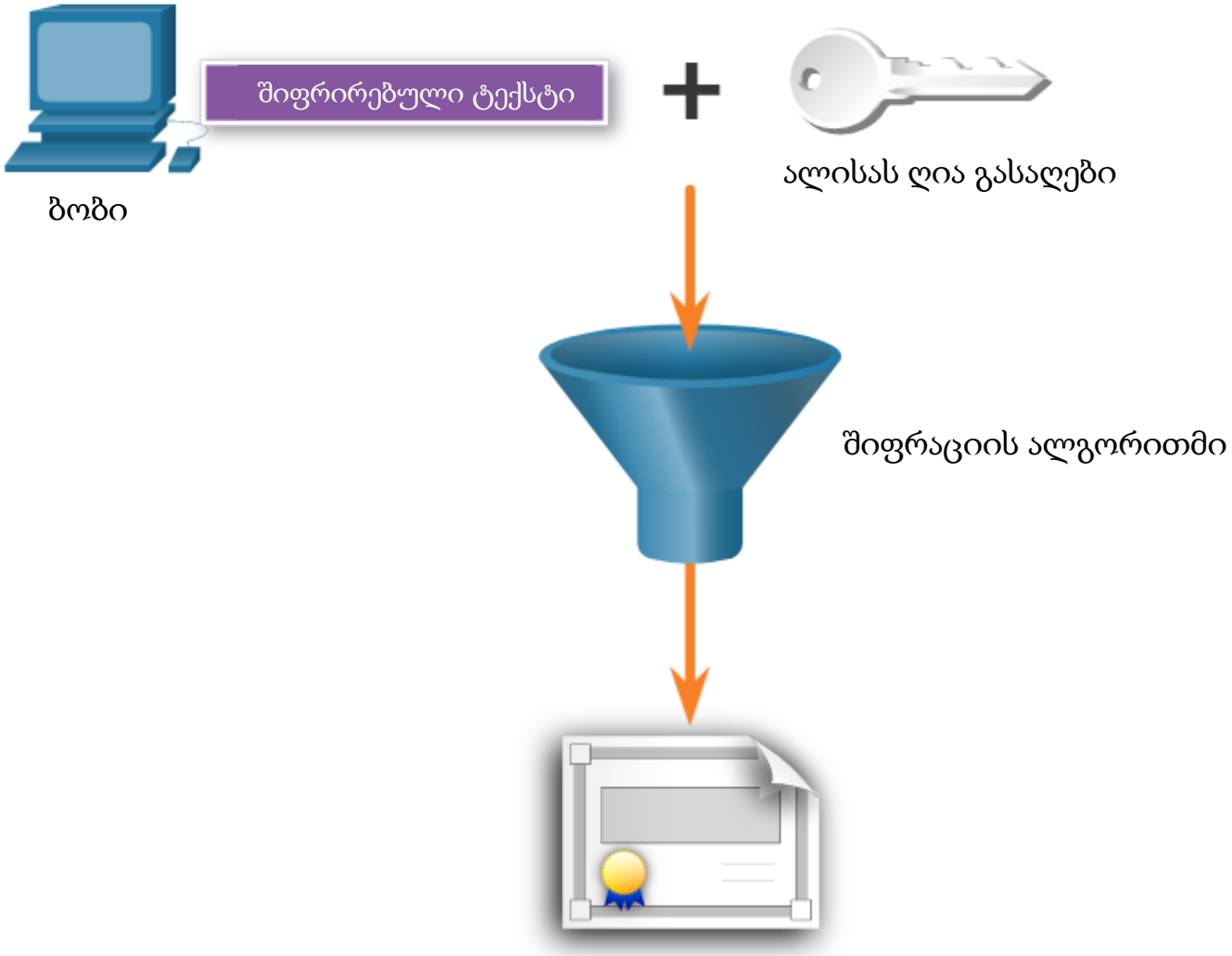


დახურული გასაღები (შიფრაცია) + ღია გასაღები (დეშიფრაცია) = აუთენტიკაცია

დახურულ გასაღებს + ღია გასაღები = აუთენტიკაციას
ბობი ითხოვს ალისას ღია გასაღებს

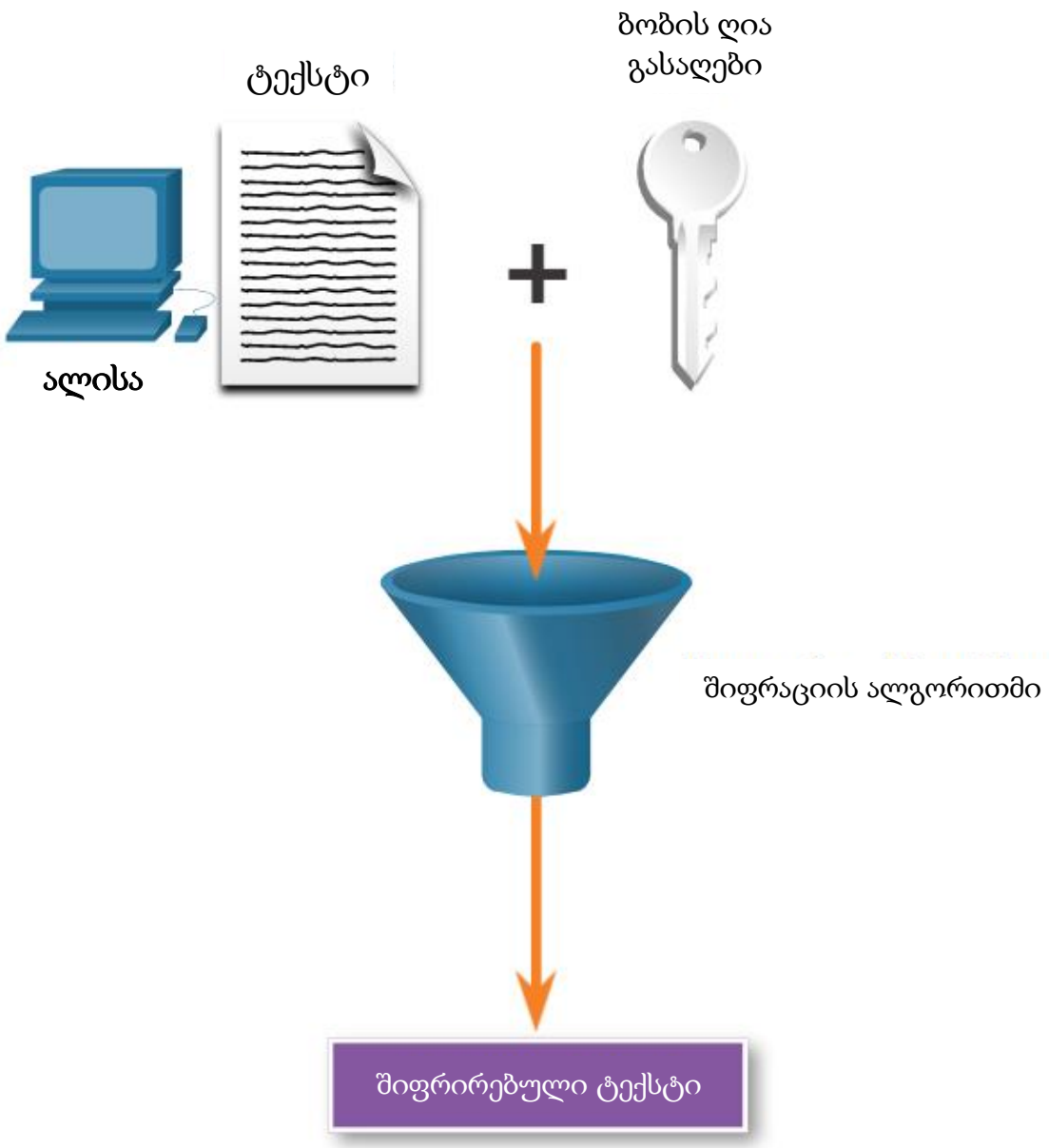
ბობს სურს დარწმუნდეს იმაში, რომ შეტყობინება ნამდვილად ალისასგან მომდინარეობს. ის ითხოვს და იღებს ალისას ღია გასაღებს

დახურულ გასაღებს + ღია გასაღები = აუთენტიკაციას
ბობი ახდენს შეტყობინების დეშიფრაციას ღია გასაღების გამოყენებით

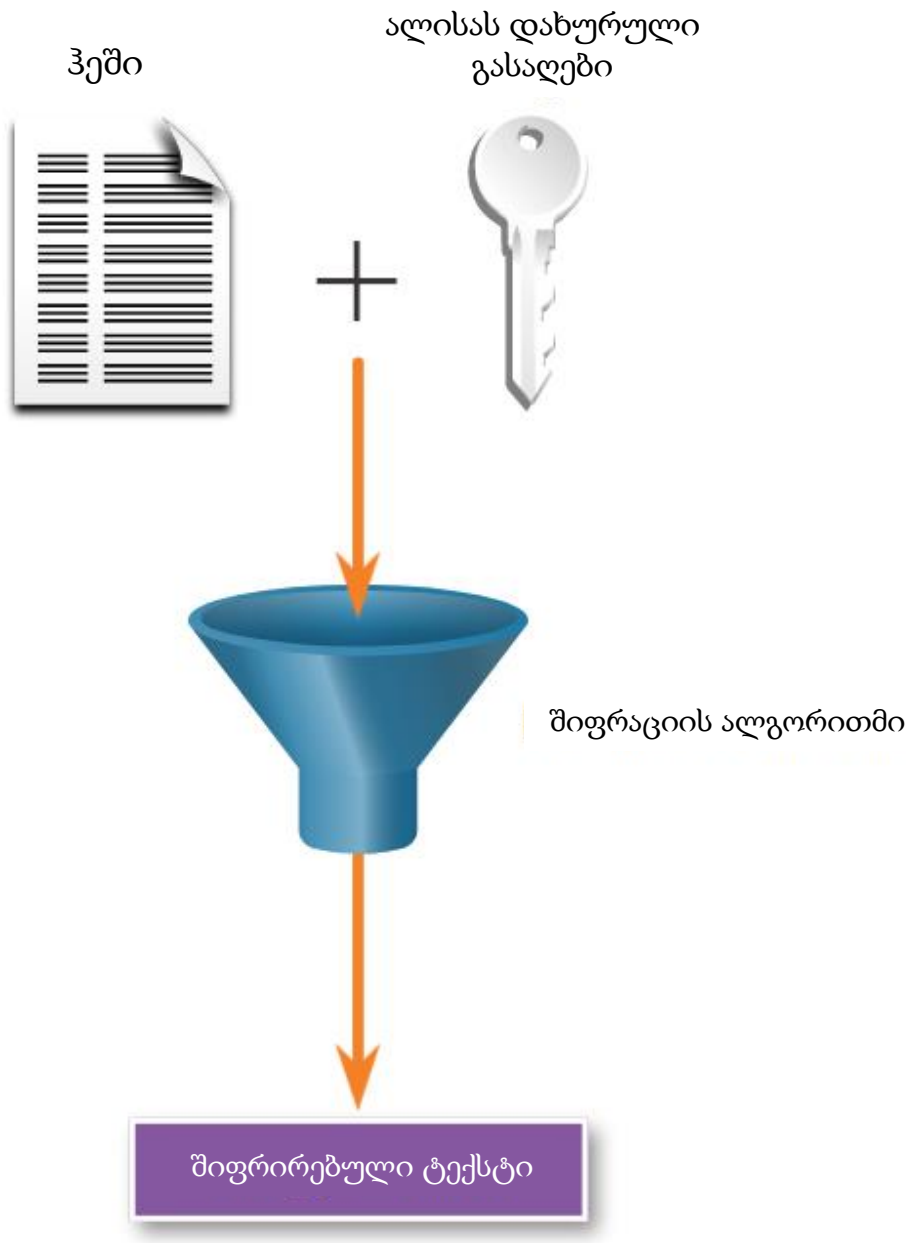


ბობი ღია გასაღებს იყენებს შეტყობინების წარმატებულად დეშიფრაციისთვის და იმის დასადასტურებლად, რომ შეტყობინება მომდინარეობს ალისასგან

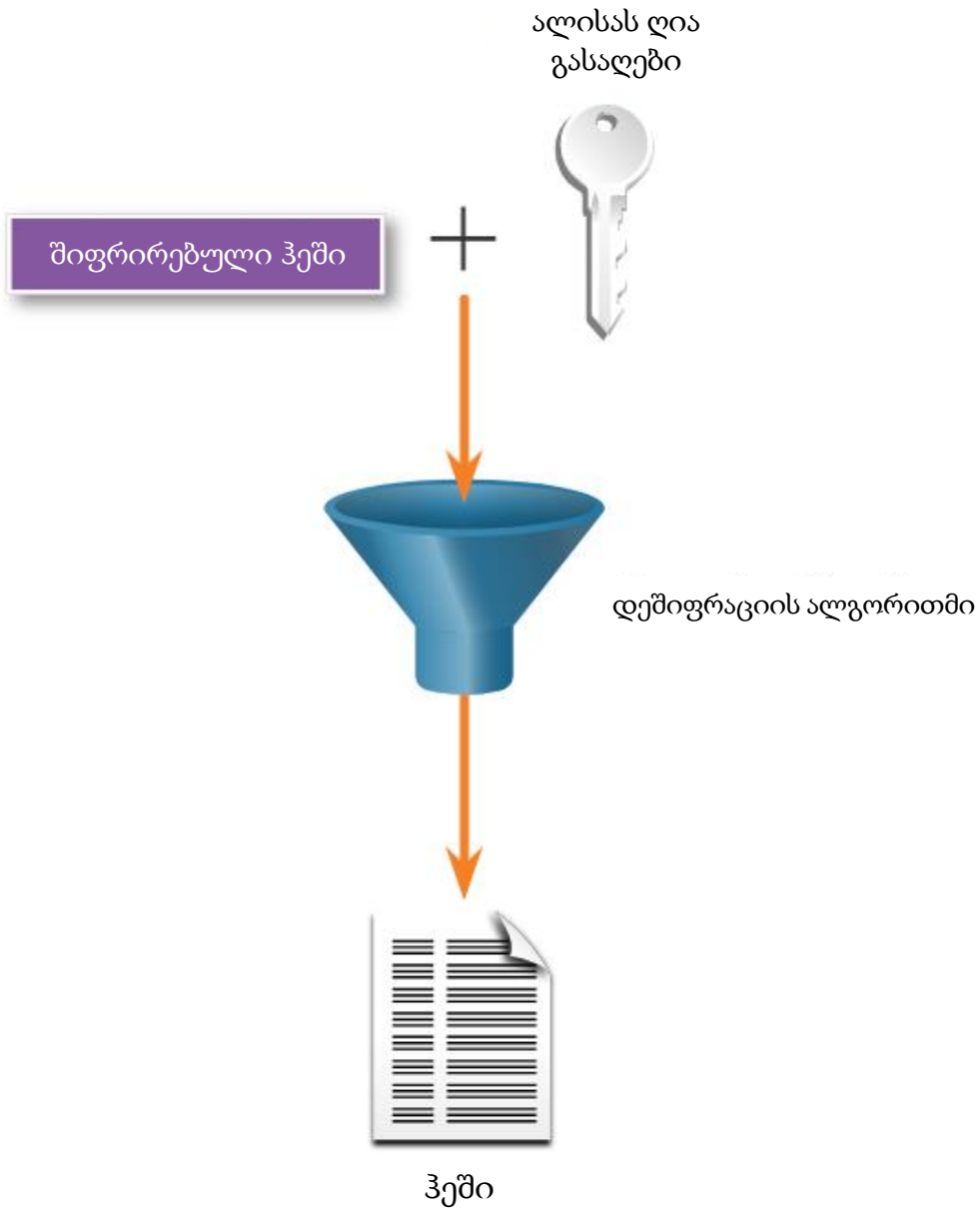
ასიმეტრიული ალგორითმები -
ალისა შიფრავს შეტყობინებას ბობის ღია გასაღების გამოყენებით



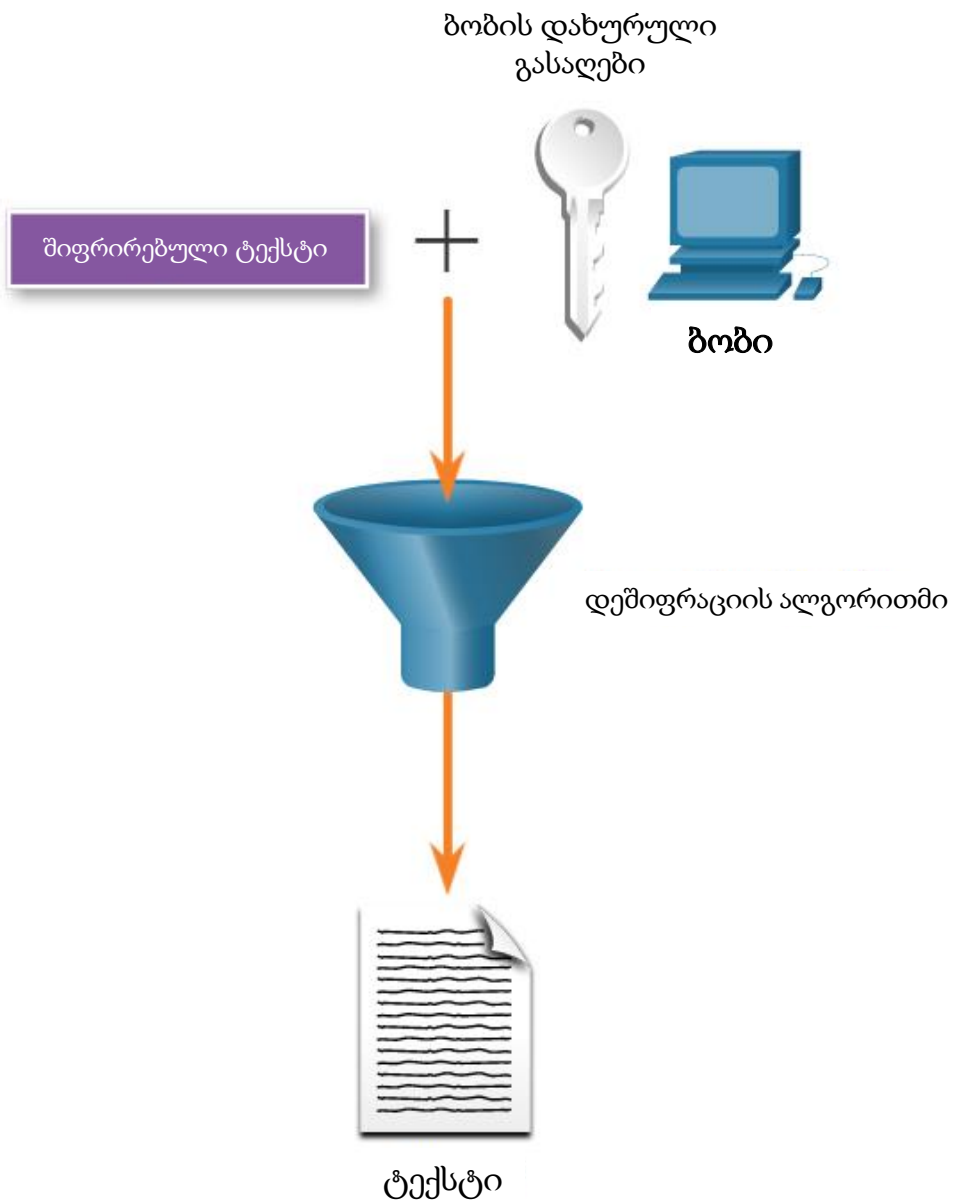
ასიმეტრიული ალგორითმები -
ალისა შიფრავს ჰეშს თავისი დახურული გასაღების გამოყენებით



ასიმეტრიული ალგორითმები - ბობი იყენებს ალისას ღია გასაღებს ჰეშის დეშიფრაციისთვის



ასიმეტრიული ალგორითმები -
ბობი იყენებს თავის დახურულ გასაღებს შეტყობინების დეშიფრაციისთვის



ასიმეტრიული ალგორითმების ტიპები - ასიმეტრიული შიფრაციის ალგორითმები

ასიმეტრიული შიფრაციის ალგორითმი	გასაღების სიგრძე (ბიტებში)	აღწერა
DH	512, 1024, 2048, 3072, 4096	დიფი-ჰელმანის (Diffie-Hellman) ალგორითმი არის ღია გასაღების ალგორითმი, რომელიც შეიქმნა 1976 წელს ვაიტფილდ დიფისა და მარტინ ჰელმანის მიერ. ის აძლევს საშუალებას ორ მხარეს, რომ შეთანხმდნენ ერთ გასაღებზე, რომელსაც გამოიყენებენ ისინი იმ შეტყობინებების დასაშიფრად, რომლის გაგზავნაც სურთ ერთმანეთთან. მოცემული ალგორითმის უსაფრთხოება დამოკიდებულია “ვარაუდზე”, რომ ადვილია რიცხვის აყვანა გარკვეულ ხარისხში, მაგრამ რთულია იმის გამოთვლა თუ რომელი ხარისხი იქნა გამოყენებული, მოცემული რიცხვისა და შედეგის მიხედვით.
ციფრული ხელმოწერის სტანდარტი (DSS) და ციფრული ხელმოწერის ალგორითმი (DSA)	512 - 1024	DSS შეიქმნა NIST-ის მიერ და ზუსტად განსაზღვრავს DSA-ს, როგორც ალგორითმს ციფრული ხელმოწერებისათვის. DSA არის ღია გასაღების ალგორითმი, რომელიც დაფუძნებულია ElGamal ხელმოწერის სქემაზე. ხელმოწერის შექმნის სიჩქარე RSA-ს მსგავსია, მაგრამ 10-40-ჯერ ნელი დადასტურებაში (verification).
RSA შიფრაციის ალგორითმი	512-დან 2048-მდე	შეიქმნა მასაჩუსეტსის ტექნოლოგიურ უნივერსიტეტში, რონ რივესტის (Ron Rivest), ადი შამირის (Adi Shamir) და ლეონარდ ადლემანის (Leonard Adleman) მიერ, 1977 წელს. ის არის ალგორითმი ღია-გასაღებით კრიპტოგრაფიისთვის, რომელიც დაფუძნებულია ძალიან დიდი რიცხვების მამრავლებად დაშლის მიმდინარე სირთულეებზე. ეს არის პირველი ალგორითმი, ცნობილი როგორც ხელმოწერისა და შიფრაციისთვის შესაფერისი და ერთ-ერთი პირველი დიდი წარმატებებიდან, ღია გასაღების კრიპტოგრაფიაში. ფართოდ გამოიყენება ელექტრონული კომერციის პროტოკოლებში და ითვლება დაცულად, საკმარისად გრძელი გასაღებებისა და თანამედროვე რეალიზაციებში გამოყენების გათვალისწინებით.

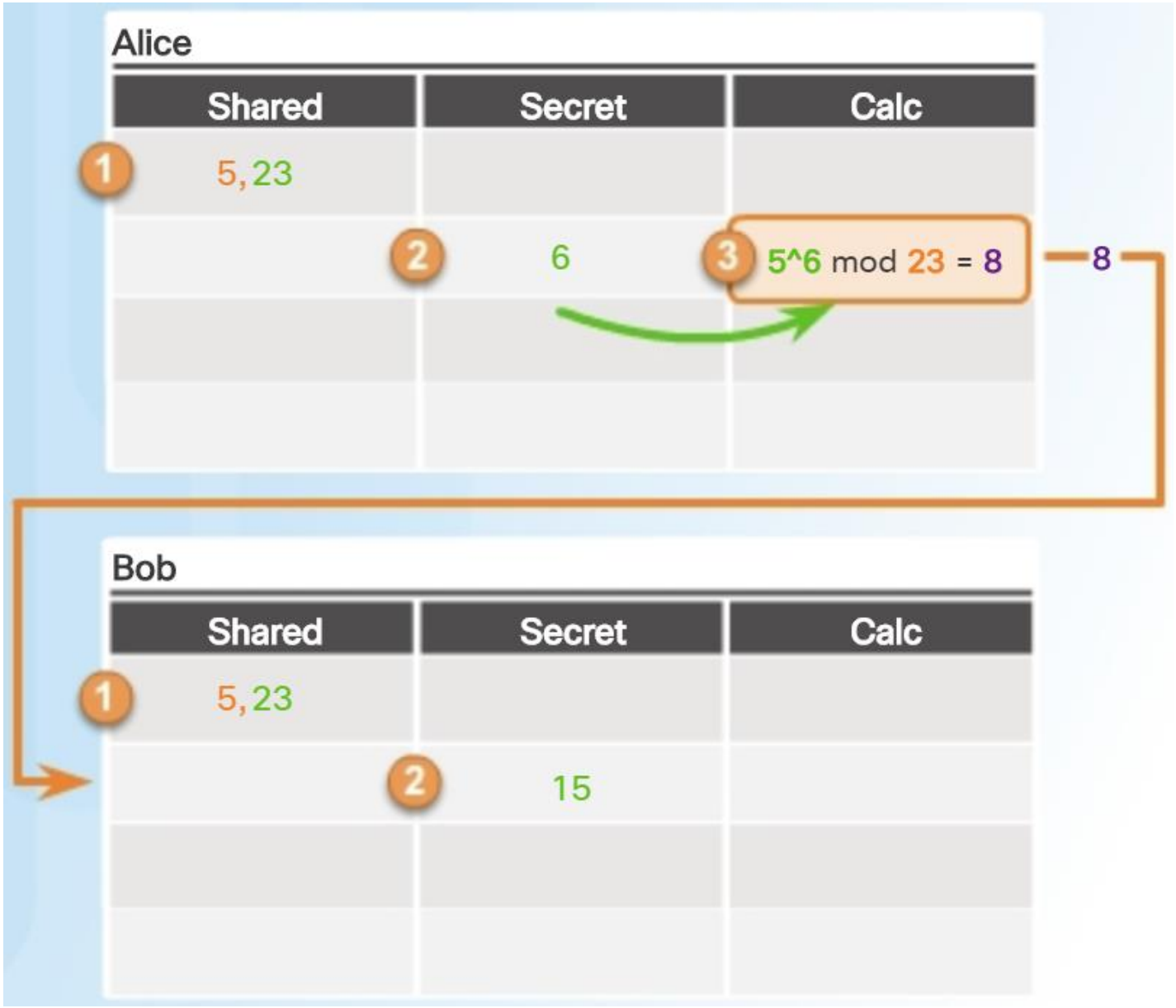
ასიმეტრიული ალგორითმების ტიპები - ასიმეტრიული შიფრაციის ალგორითმები

ასიმეტრიული შიფრაციის ალგორითმი	გასაღების სიგრძე (ბიტებში)	აღწერა
ElGamal	512 - 1024	ასიმეტრიული გასაღებით შიფრაციის ალგორითმი ღია-გასაღებით კრიპტოგრაფიისთვის, რომელიც დაფუძნებულია Diffie-Hellman-ის გასაღების ურთიერთშეთანხმებაზე. წარმოდგენილია Taher ElGamal-ის მიერ 1984 წელს და გამოიყენება GNU Privacy Guarg პროგრამულ უზრუნველყოფაში, PGP-ში და სხვა კრიპტოსისტემებში. ElGamal-ის სისტემის ნაკლი არის ის, რომ დაშიფრული შეტყობინება ხდება ძალიან დიდი, ორიგინალ შეტყობინებაზე დაახლოებით ორჯერ მეტი, და ამ მიზეზით ის გამოიყენება მხოლოდ მცირე ზომის შეტყობინებებში, როგორიცაა საიდუმლო გასაღებები.
Elliptical curve techniques - ელიფსური მრუდის ტექნიკები	224 ან მაღალი	ელიფსური მრუდის კრიპტოგრაფია გამოიგონა Neil Koblitz-მა და Victor Miller-მა შუა 1980-იან წლებში. შეიძლება იქნას გამოყენებული მრავალ კრიპტოგრაფიულ სისტემასთან შეწყობისთვის, როგორიცაა Diffie-Hellman ან ElGamal. ელიფსური მრუდით კრიპტოგრაფიის მთავარი უპირატესობა არის ის, რომ გასაღებები შეიძლება იყოს ბევრად უფრო პატარა.

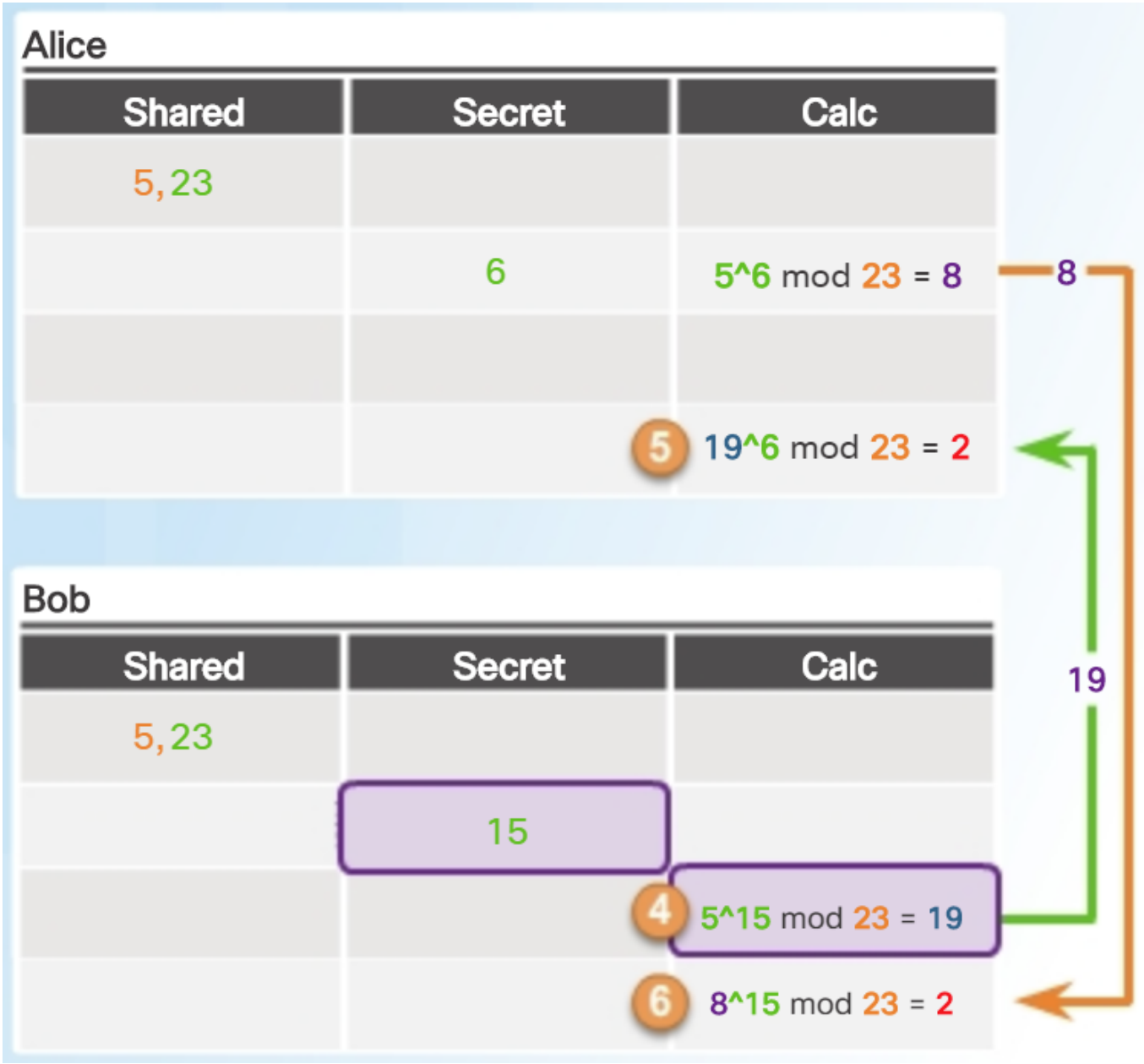
Diffie-Hellman გასაღების გაცვლა - Diffie-Hellman ალგორითმი

DH-ის მახასიათებლები	
აღწერა	Diffie-Hellman ალგორითმი
გამოშვების დრო	1976
ალგორითმის ტიპი	ასიმეტრიული
გასაღების ზომა (ბიტებში)	512, 1024, 2048, 3072, 4096
სიჩქარე	ნელი
გატეხვის დრო (ვივარაუდოთ, რომ კომპიუტერს შეუძლია 255 გასაღების ცდა წამში)	უცნობია, მაგრამ მიჩნეულია დაცულად 2048 ბიტიანი ან უფრო მაღალი სიგრძის გასაღების გამოყენების შემთხვევაში
რესურსების მოხმარება	საშუალო

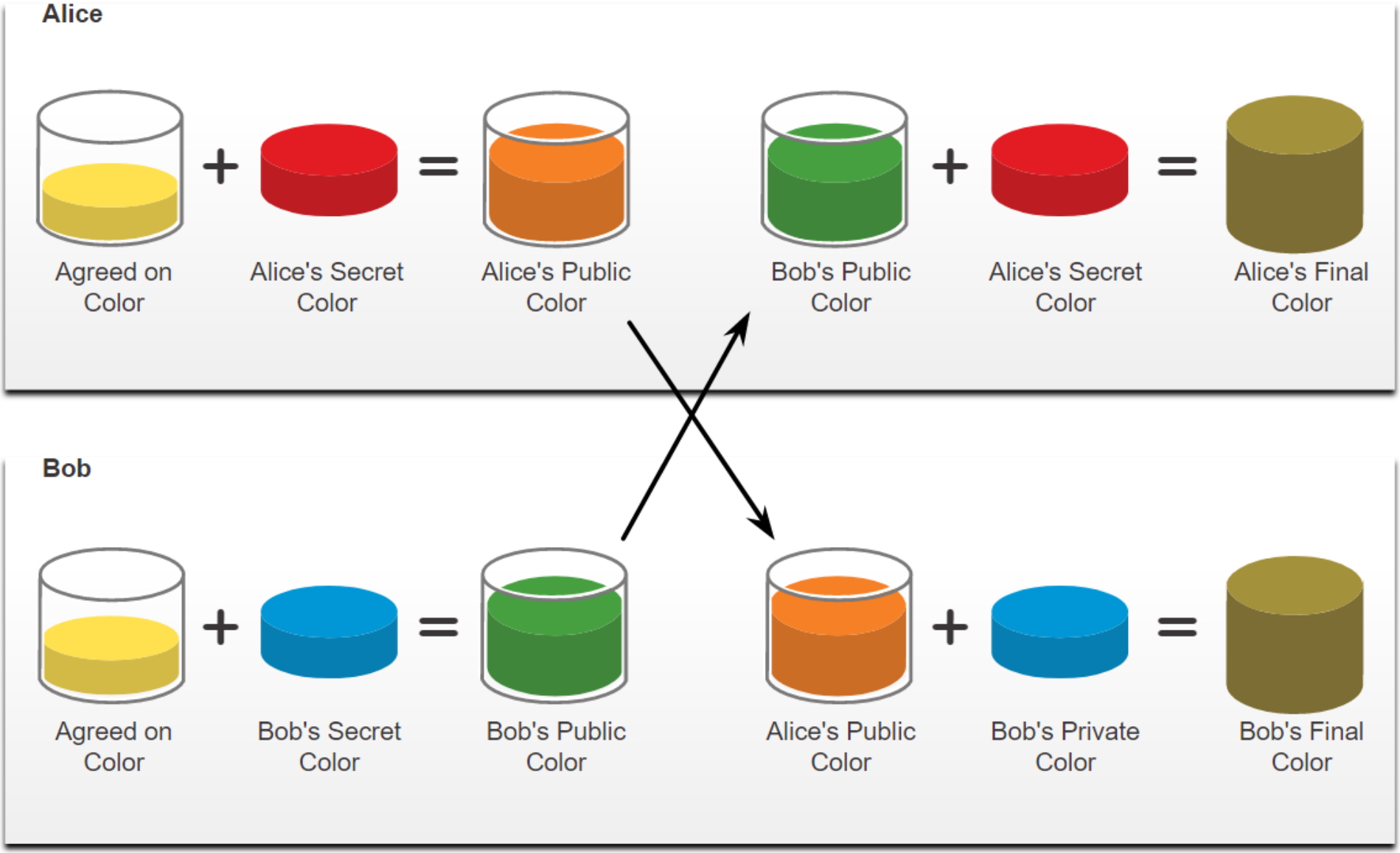
DH ოპერაცია (1-3 ეტაპები)



DH ოპერაცია (4-6 ეტაპები)



Diffie-Hellman



RSA ალგორითმის სქემა

1. მოითხოვება ორი ძალიან დიდი მარტივი რიცხვი “p” და “q”;
2. გადაამრავლეთ ზემოთ მოცემული მარტივი რიცხვები ერთმანეთზე, რათა იპოვოთ n, მოდული შიფრაციისა და დეშიფრაციისთვის, სხვა სიტყვებით რომ ვთქვათ n = p * q;
3. გამოთვალეთ ეილერის ინდიკატორი Φ = (p – 1) * (q – 1)
4. აირჩიეთ შემთხვევითი მთელი რიცხვი “e”, ანუ შიფრაციის გასაღები და გამოთვალეთ “d” დეშიფრაციის გასაღები ამგვარად, d x e = 1 mod Φ
5. “e” და “n” გამოაცხადეთ ღიად (public); ის საიდუმლოდ შეინახავს “Φ” და “d” -ს

RSA ალგორითმის მაგალითი
თემატური კვლევა:
ალისა თავისთვის ქმნის გასაღებთა წყვილს. ის ირჩევს p = 17 და q = 11. გამოსათვლელია ქვემოთ მოცემული მნიშვნელობები.
A - გამოვთვალოთ
n = ? Φ = ?
B - შემდეგ ის ირჩევს e = 7; d = ?
C - ვნახოთ როგორ შეუძლია ბობს „88“ შეტყობინების გაგზავნა ალისასთვის, თუ მან იცის e და n

A - ამოხსნა:
როგორც ვიცით:
n = p * q; n = 17 *11; n =187

მოდით ვიპოვოთ Φ
Φ= (p-1) * (q-1)
Φ= (17-1) * (11-1)
Φ= (16) * (10); Φ=160

RSA ალგორითმის სქემა

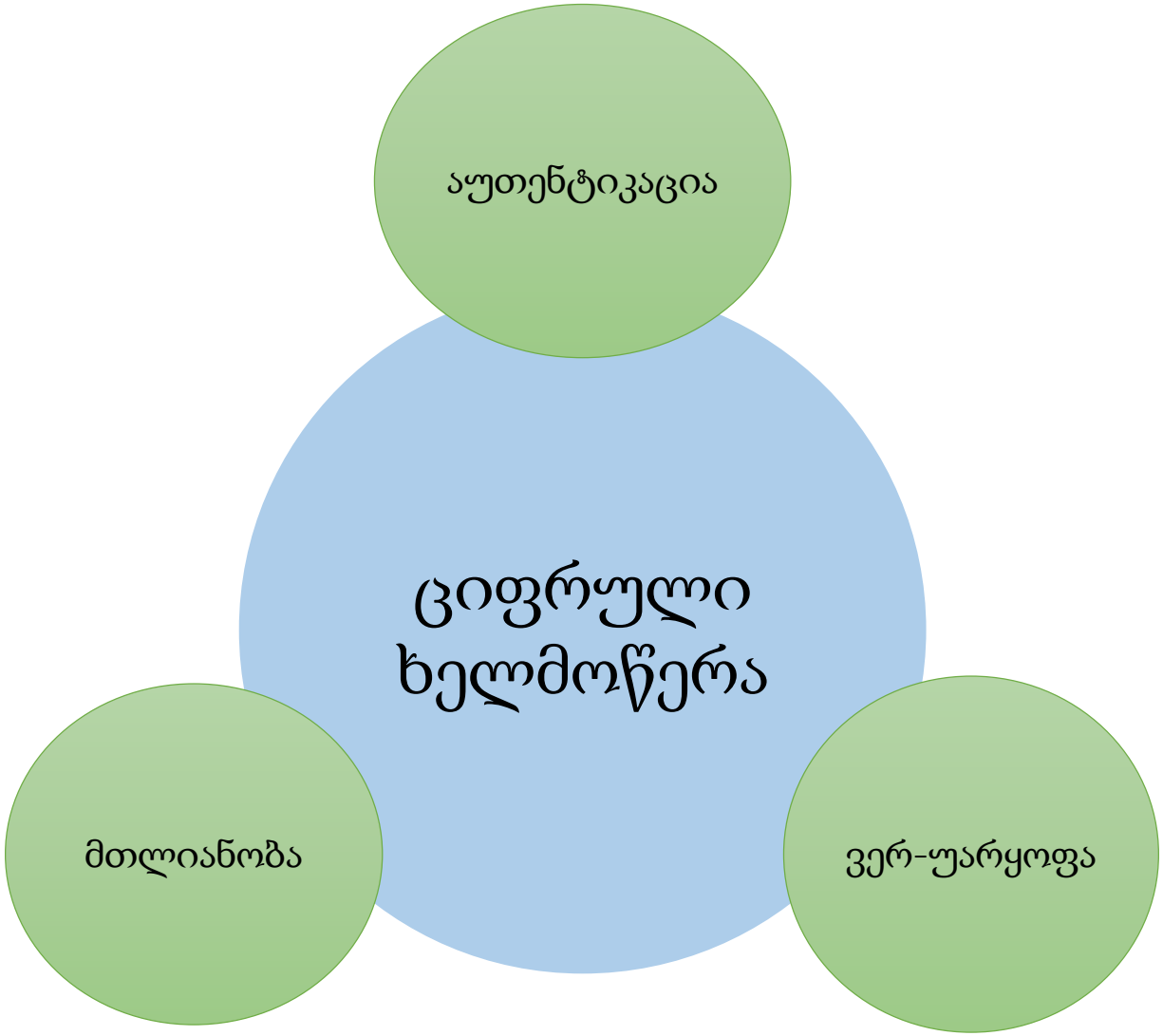
B - ამოხსნა

თუ e=7, მოდით გამოვთვალოთ d-ს მნიშვნელობა
როგორც ვიცით:
$d \times e = 1 \bmod \Phi$
$d = e^{-1} \bmod \Phi$
$d = 7^{-1} \bmod 160$
$d = 23$

C - ამოხსნა

ალისას დახურული (private) გასაღები იქნება (d,p,q) = (23,17,11)
ალისას ღია (public) გასაღები იქნება (e,n) = (7, 187)
ალისა თავის ღია გასაღებს უზიარებს ბობს. ბობი მოახდენს პაკეტების შიფრაციას ალისას ღია გასაღების გამოყენებით და დაშიფრულ შეტყობინებას გაუგზავნის მას.
როგორც ვიცით: $C=M^e \bmod n$, სადაც "C" არის დაშიფრული შეტყობინება, ხოლო "M" - შეტყობინება
$C=M^e \bmod n$
$C=(88)^7 \bmod 187$
$C=11$
ბობი გააგზავნის „11"-ს ალისასთან. ორიგინალი შეტყობინების მისაღებად, ალისა მოახდენს შიფრის დეშიფრაციას თავისი დახურული (private) გასაღებით
როგორც ვიცით:
$M=C^d \bmod n$
$M=(11)23 \bmod 187$
$M= 88$

ციფრული ხელმოწერები - ციფრული ხელმოწერების გამოყენება - ციფრული ხელმოწერების მიერ უზრუნველყოფილი სერვისები



ციფრული ხელმოწერების გამოყენება - ციფრული ხელმოწერის თვისებები

ციფრული ხელმოწერის შექმნის პროცესები - ალისა ქმნის შეტყობინების პროფილს და შიფრავს მას თავისი დახურული გასაღებით

ციფრული ხელმოწერის შექმნის პროცესები - ალისა აგზავნის ხელმოწერილ დოკუმენტს

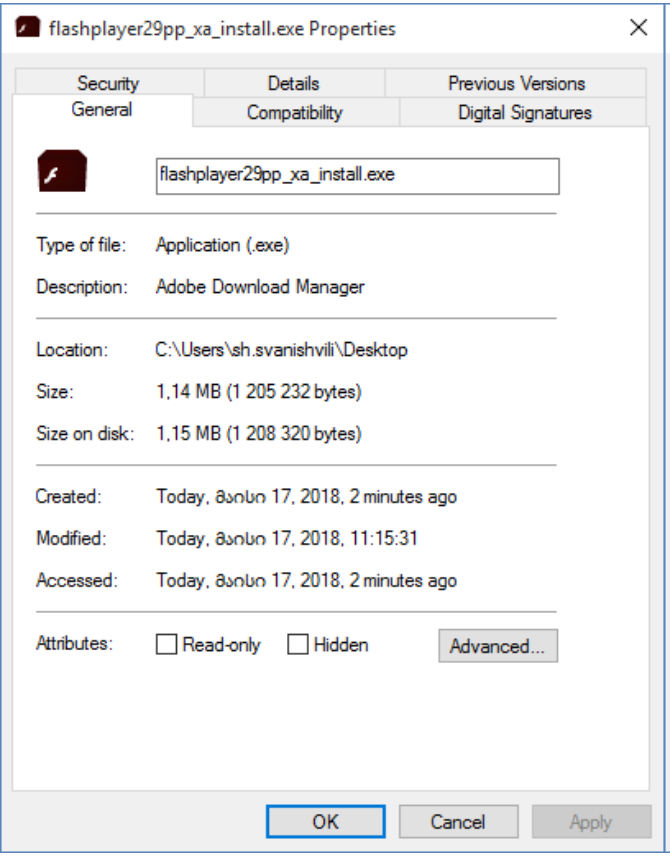
ციფრული ხელმოწერის შექმნის პროცესები - ბობი ეცნობა დოკუმენტს და ადარებს შეტყობინების პროფილს

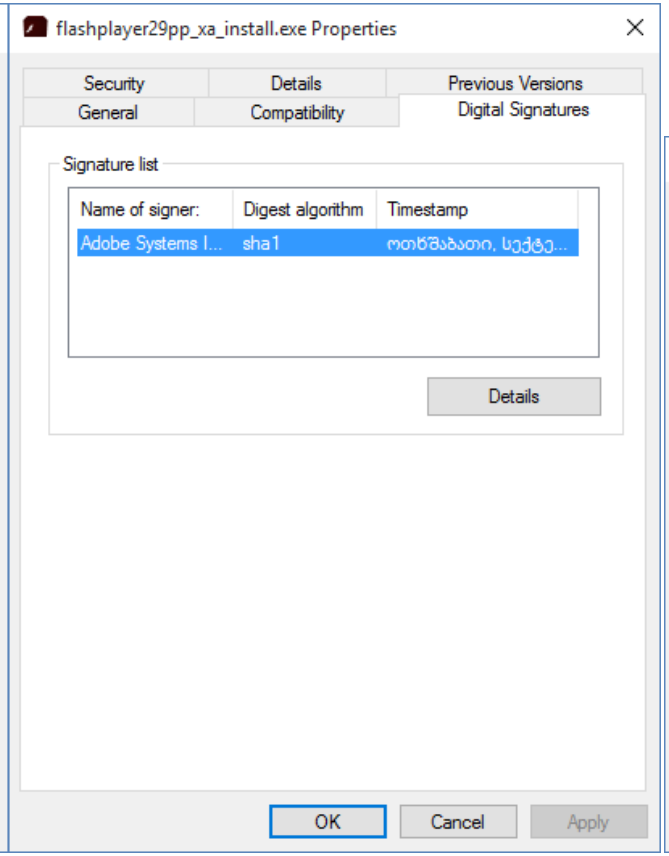
კოდის ხელმოწერა

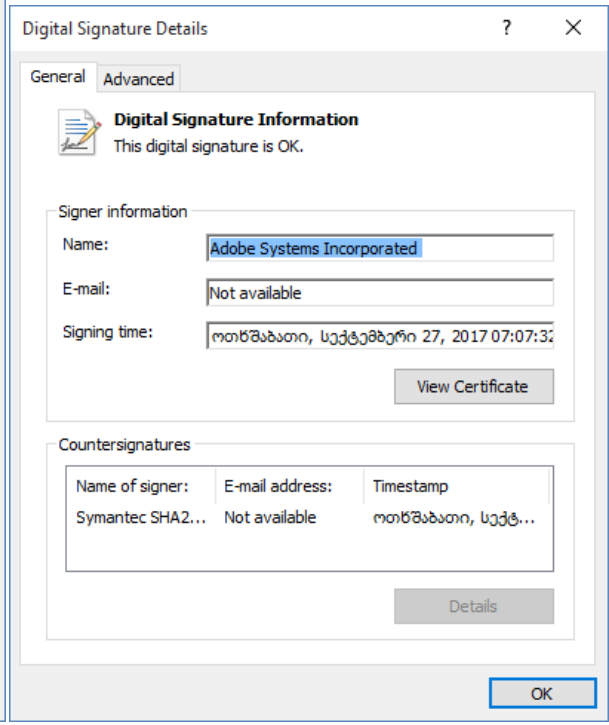
ფაილის თვისებები

ციფრული ხელმოწერების ჩანართი

ციფრული ხელმოწერის დეტალური ინფორმაცია

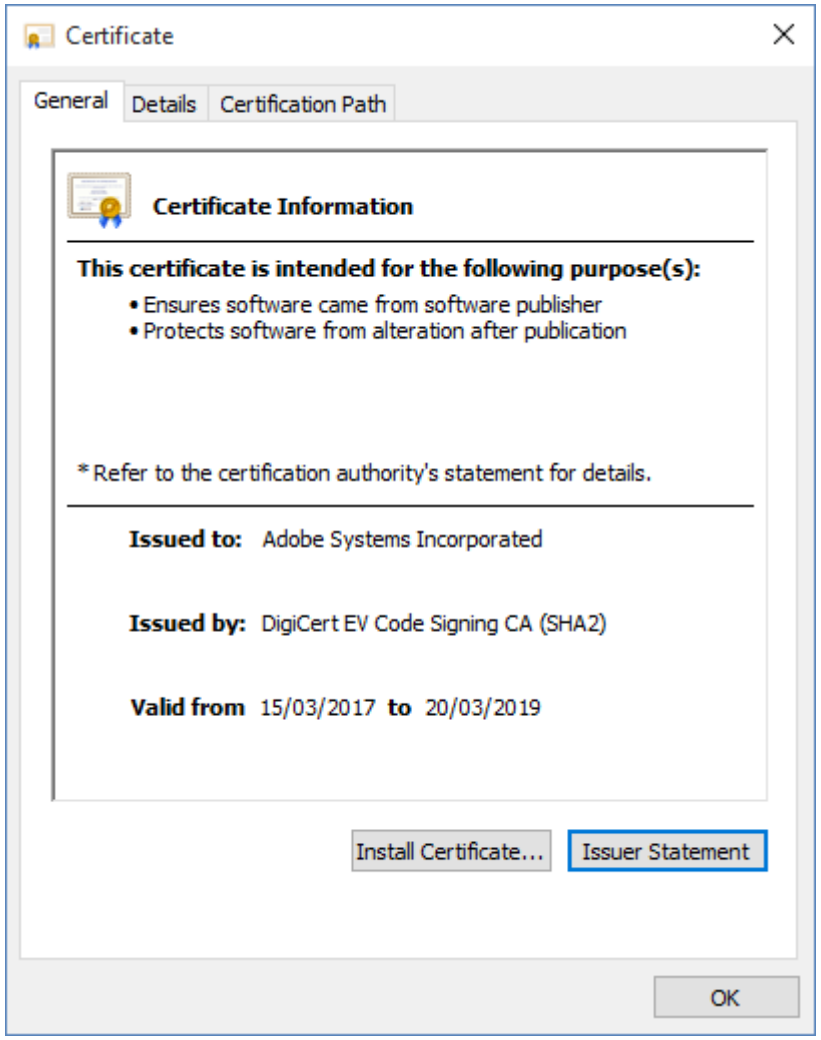




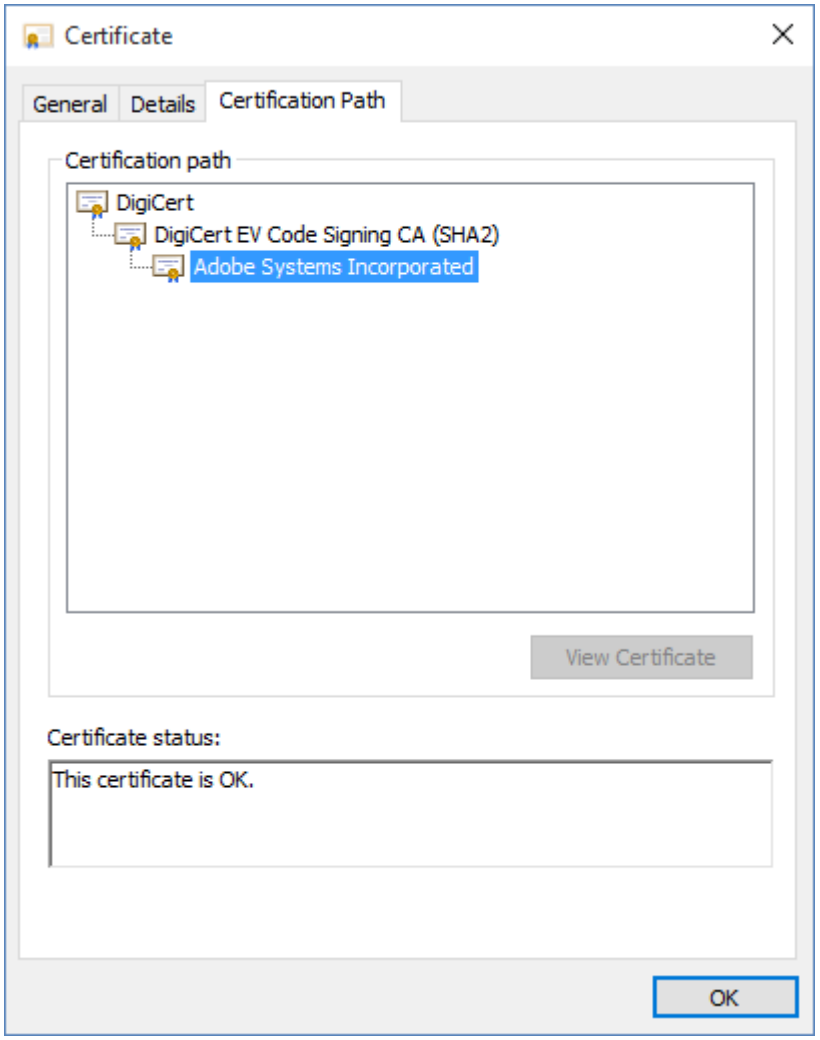


კოდის ხელმოწერა

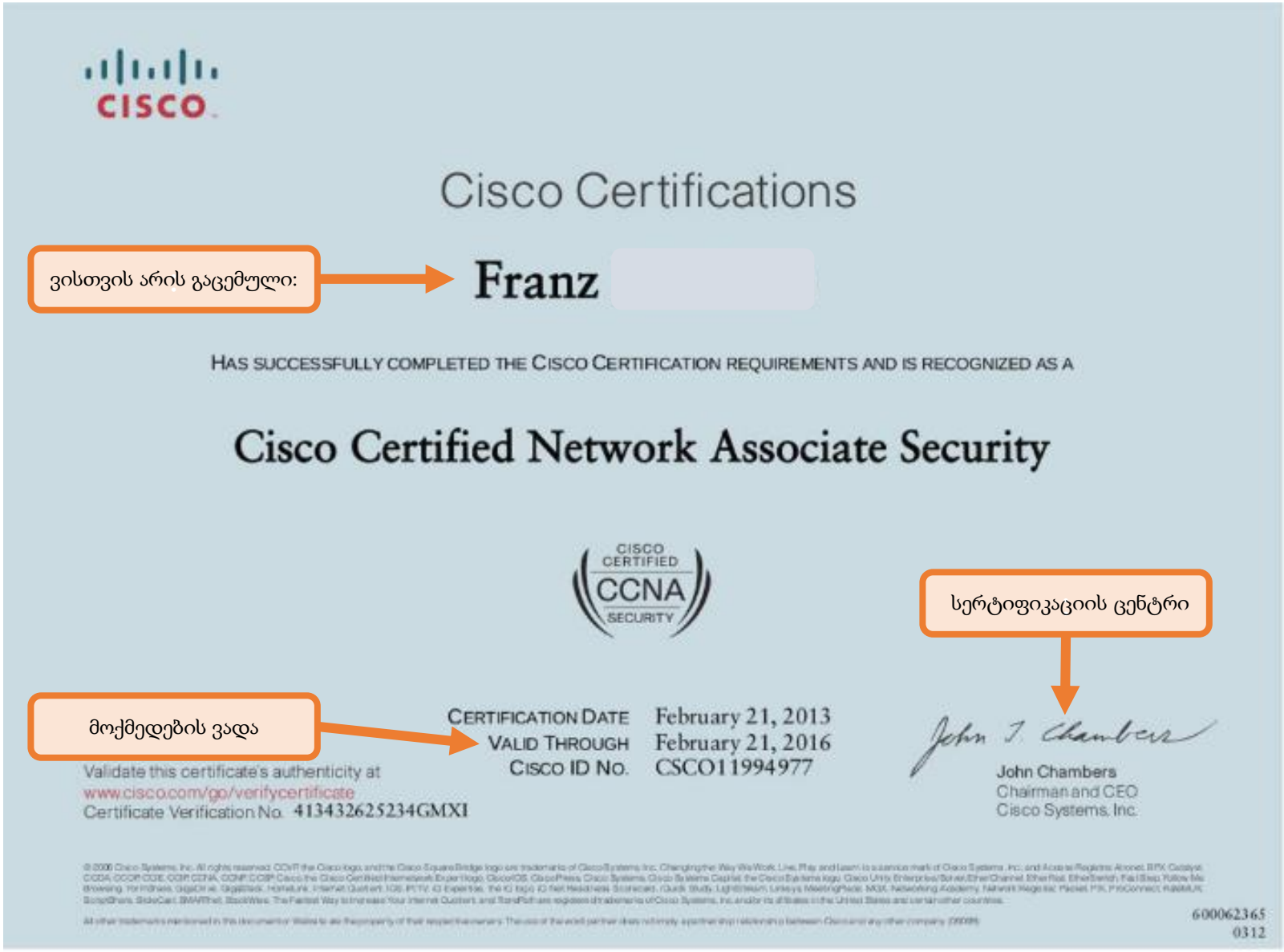
ციფრული სერტიფიკატის ინფორმაცია



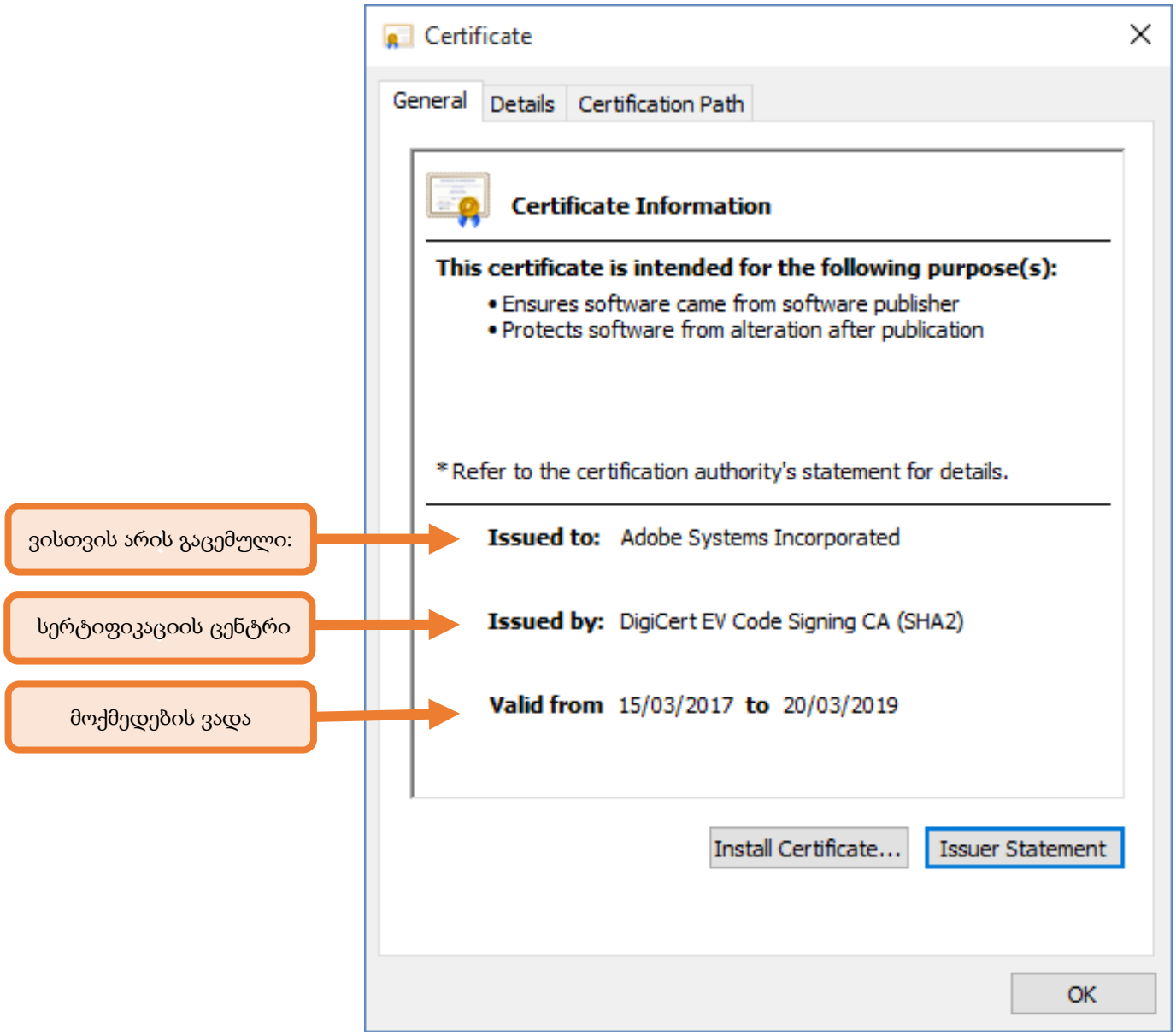
გზა ციფრულ სერტიფიკატამდე



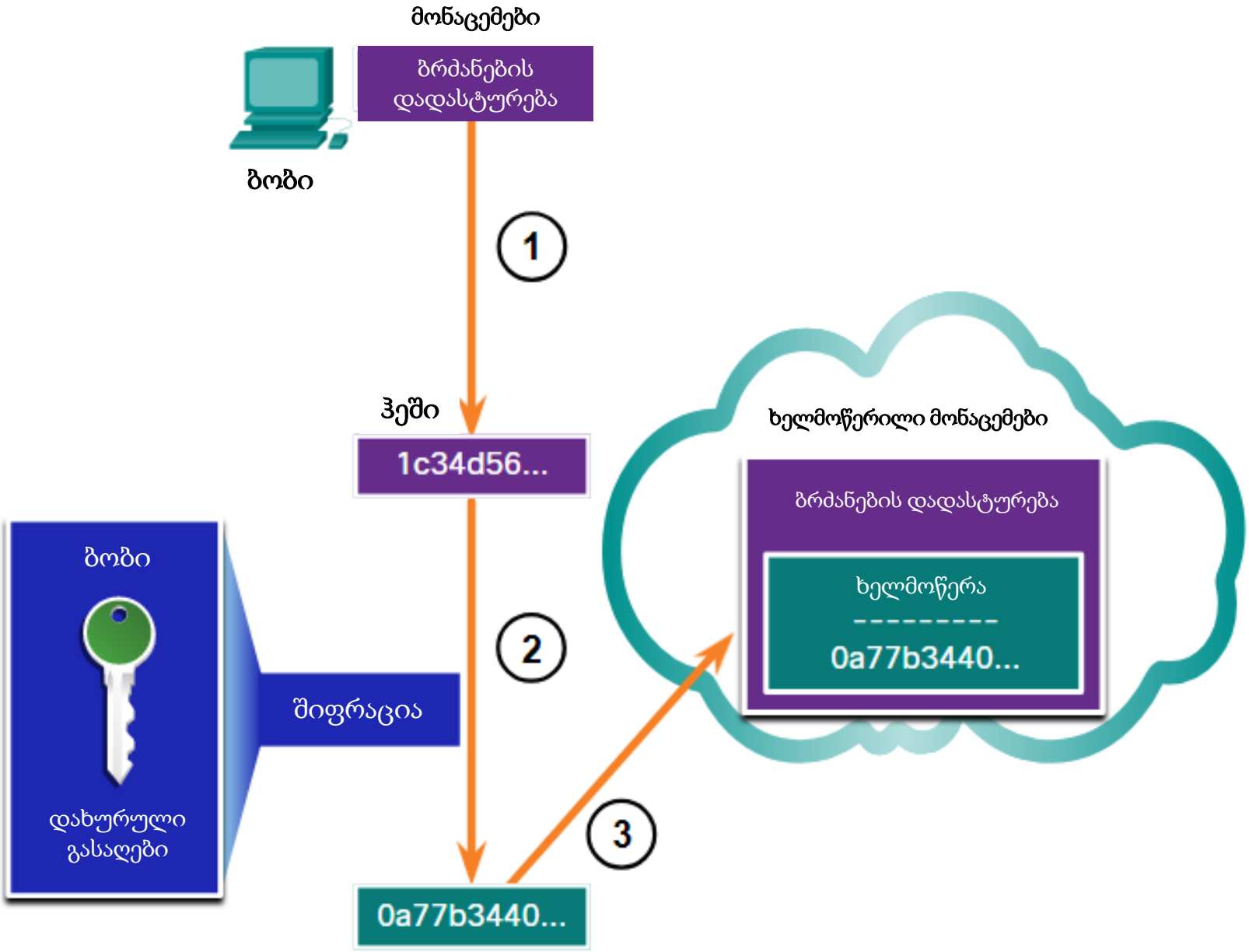
ციფრული სერტიფიკატები - ფიზიკური CCNA უსაფრთხოების სერტიფიკატი



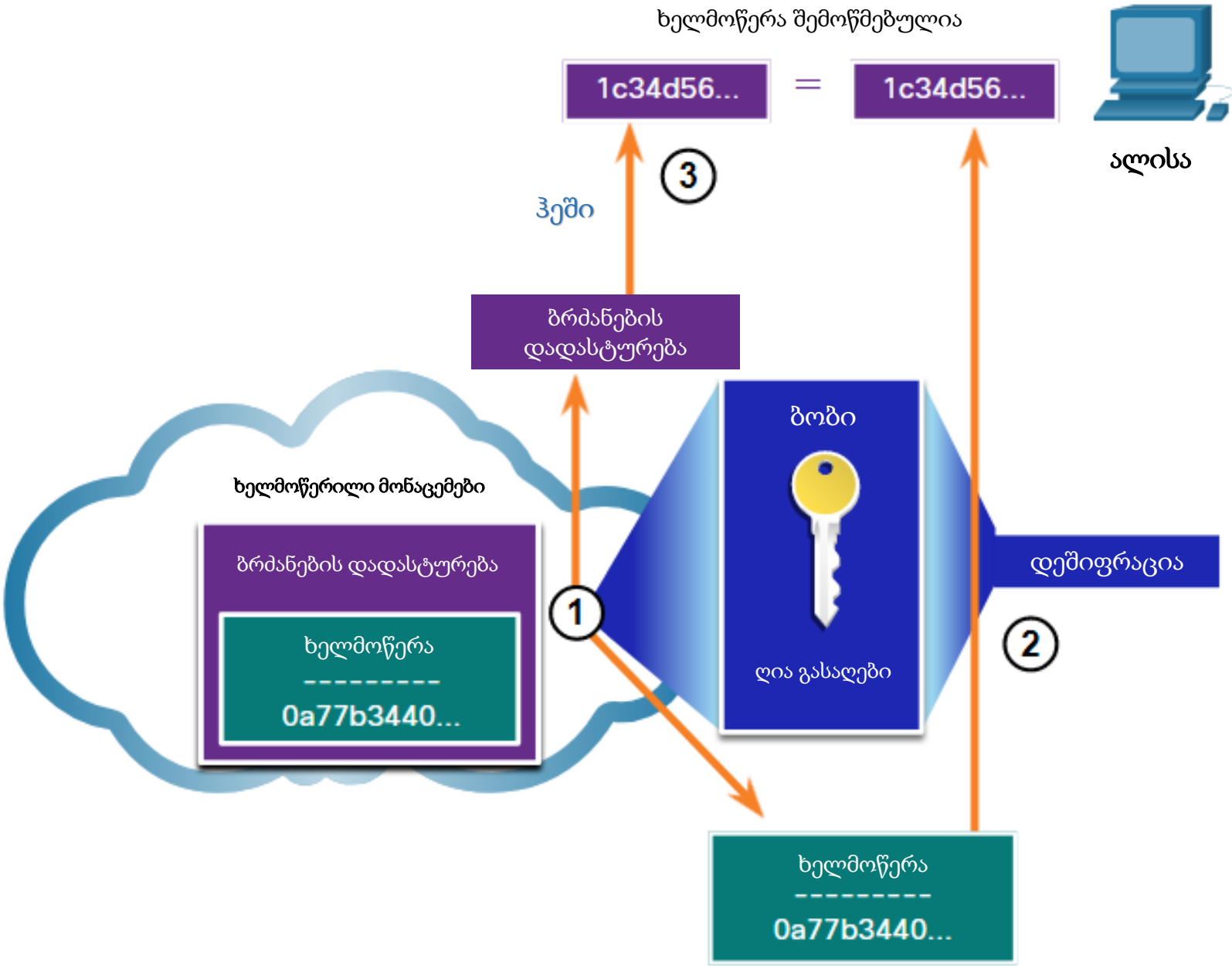
ციფრული სერტიფიკატები - ციფრული სერტიფიკატის ინფორმაცია



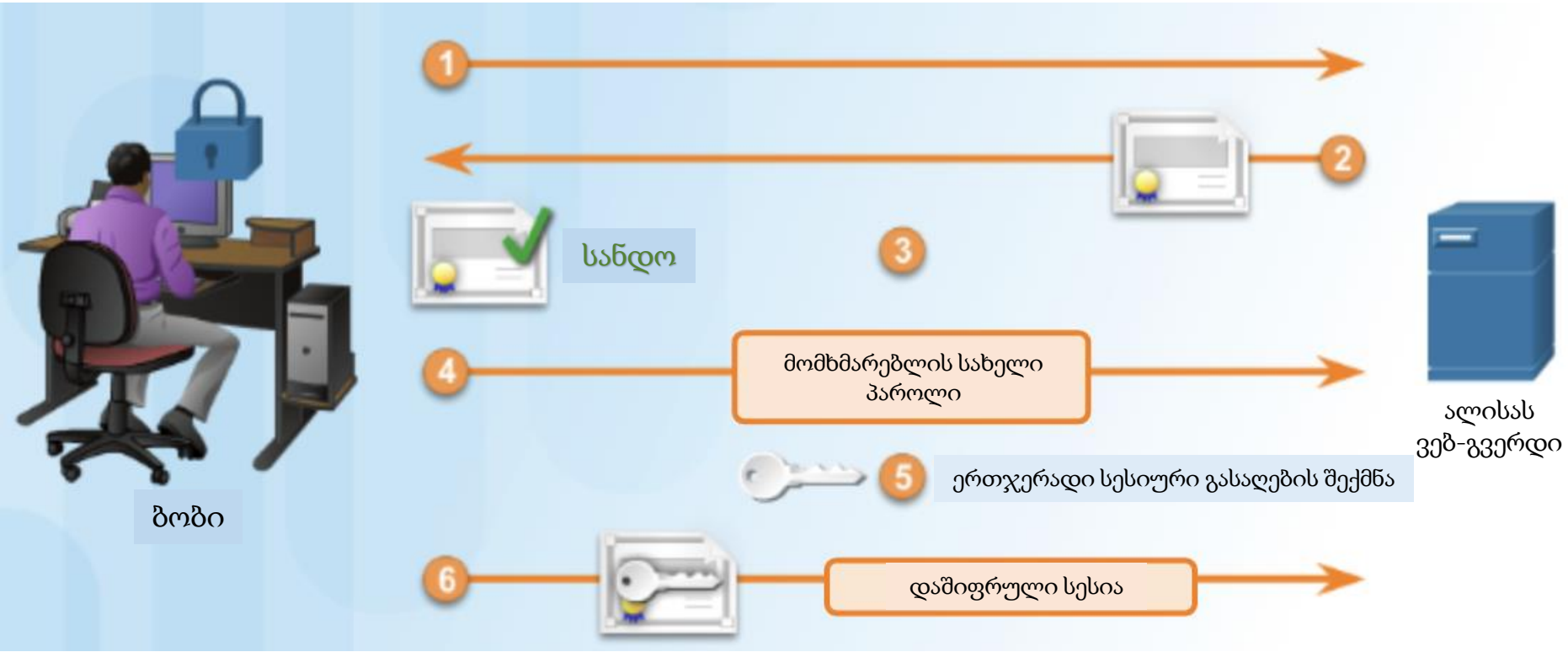
ციფრული სერტიფიკატების გამოყენება - ციფრული სერტიფიკატის გაგზავნა



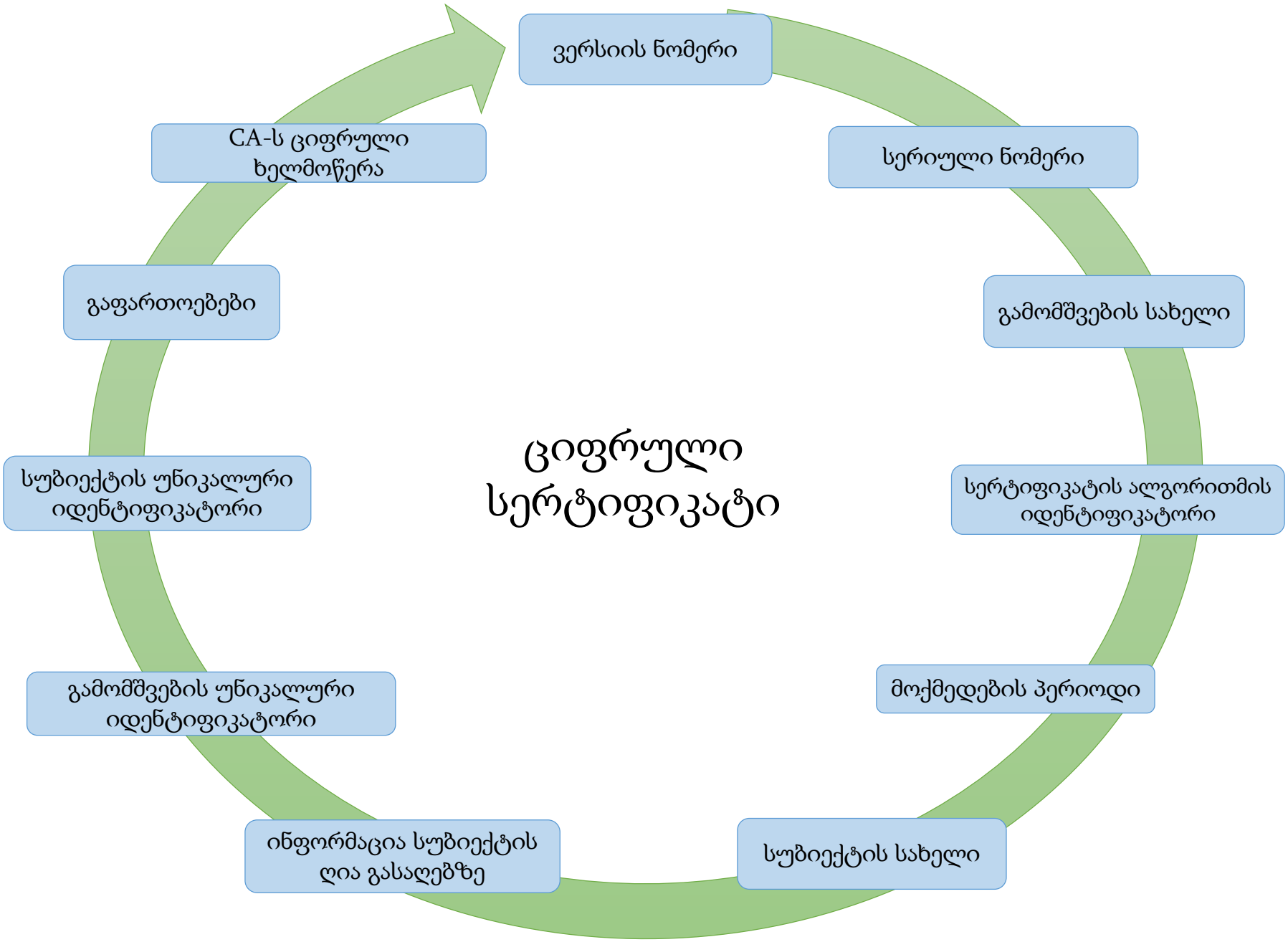
ციფრული სერტიფიკატების გამოყენება - ციფრული სერტიფიკატის მიღება



ციფრული სერტიფიკატების გამოყენება



რა იმალება ციფრული სერტიფიკატის შიგნით?



ციფრული სერტიფიკატის ალგორითმები - DSA-ს და RSA-ს შეფასების ცხრილები

DSA-ის მახასიათებლები	
აღწერა	ციფრული ხელმოწერის ალგორითმი (DSA)
გამოშვების დრო	1994
ალგორითმის ტიპი	იძლევა ციფრულ ხელმოწერებს
უპირატესობები	ხელმოწერის შექმნა არის სწრაფი
ნაკლოვანებები	ხელმოწერის დადასტურება არის ნელი

RSA-ის მახასიათებლები	
აღწერა	Ron Riverst, Adi Shamir და Len Adleman
გამოშვების დრო	1977
ალგორითმის ტიპი	ასიმეტრიული ალგორითმი
გასაღების ზომა (ბიტებში)	512 - 2048
უპირატესობები	ხელმოწერის დადასტურება არის სწრაფი
ნაკლოვანებები	ხელმოწერის შექმნა არის ნელი

ციფრულად ხელმოწერილი Cisco-ს პროგრამული უზრუნველყოფა - ბრძანება show software Authenticity

```
R1# show software authenticity file flash:c1900-universalk9-mz.SPA.154-3.M2.bin
File Name                       : flash:c1900-universalk9-mz.SPA.154-3.M2.bin
Image type                      : Production
    Signer Information
        Common Name             : CiscoSystems
        Organization Unit       : C1900
        Organization Name       : CiscoSystems
    Certificate Serial Number   : 54D56496
    Hash Algorithm              : SHA512
    Signature Algorithm         : 2048-bit RSA
    Key Version                 : A

R1#
```

აქტივობა - კოდის ხელმოწერისა და ციფრული სერტიფიკატების შედარება

მახასიათებელი	კოდის ხელმოწერა	ციფრული სერტიფიკატები
ის არის ელექტრონული პასპორტის ექვივალენტური		☑
გამოიყენება იმ შესრულებადი ფაილების მთლიანობის შესამოწმებლად, რომლებიც გადმოწერილია მომწოდებლის ვებ-გვერდიდან	☑	
მომხმარებლებს, ჰოსტებს და ორგანიზაციებს აძლევს ინტერნეტით ინფორმაციის დაცულად გაცვლის საშუალებას		☑
გამოიყენება ორგანიზაციის ნამდვილობის შესამოწმებლად და კონფიდენციალური მონაცემების გაცვლისთვის აუცილებელი შიფრირებული კავშირის შესაქმნელად		☑
იძლევა გარანტიას, რომ კოდი ავთენტურია და მომდინარეობს მწარმოებლიდან	☑	
შესრულებადი ფაილები შეფუთულია ციფრულად ხელმოწერილი გარეკანით, რაც მომხმარებელს აძლევს ხელმოწერის შემოწმების საშუალებას, პროგრამული უზრუნველყოფის დაინსტალირებამდე	☑	
შეიძლება იქნას გამოყენებული მიმღებისთვის კონფიდენციალობის უზრუნველსაყოფად, პასუხის დაშიფვრის საშუალებით		☑

ღია გასაღების ინფრასტრუქტურის მიმოხილვა - მართვის მოწმობის PKI ანალოგია

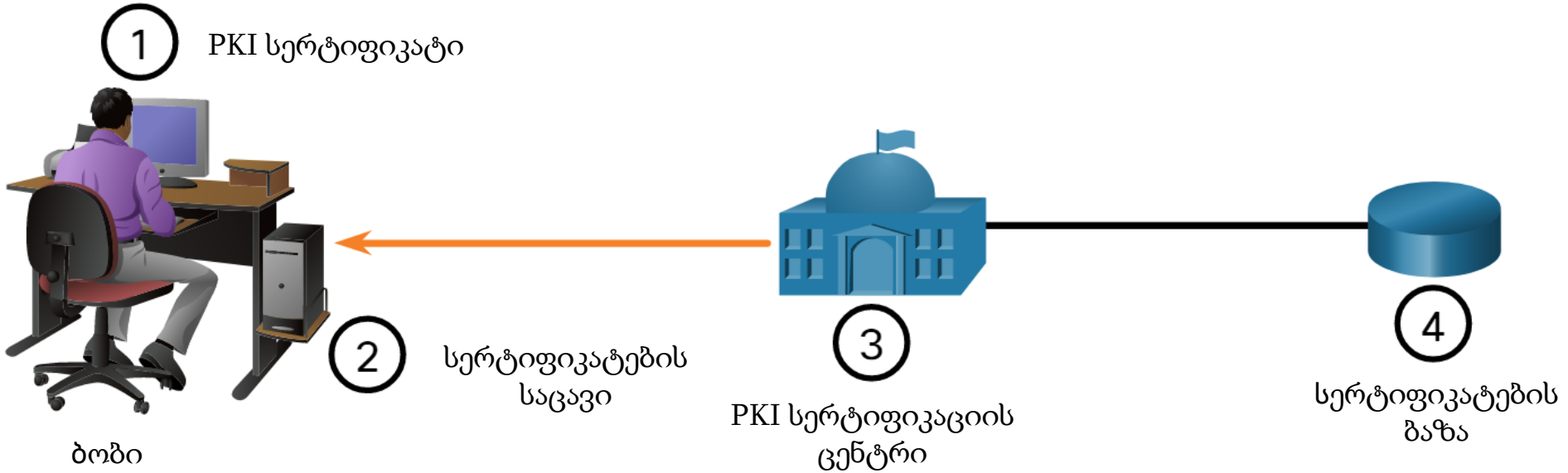
ალისა მიმართავს მართვის მოწმობის მისაღებად.

ის იღებს მართვის მოწმობას, თავისი ვინაობის დადასტურების შემდეგ.

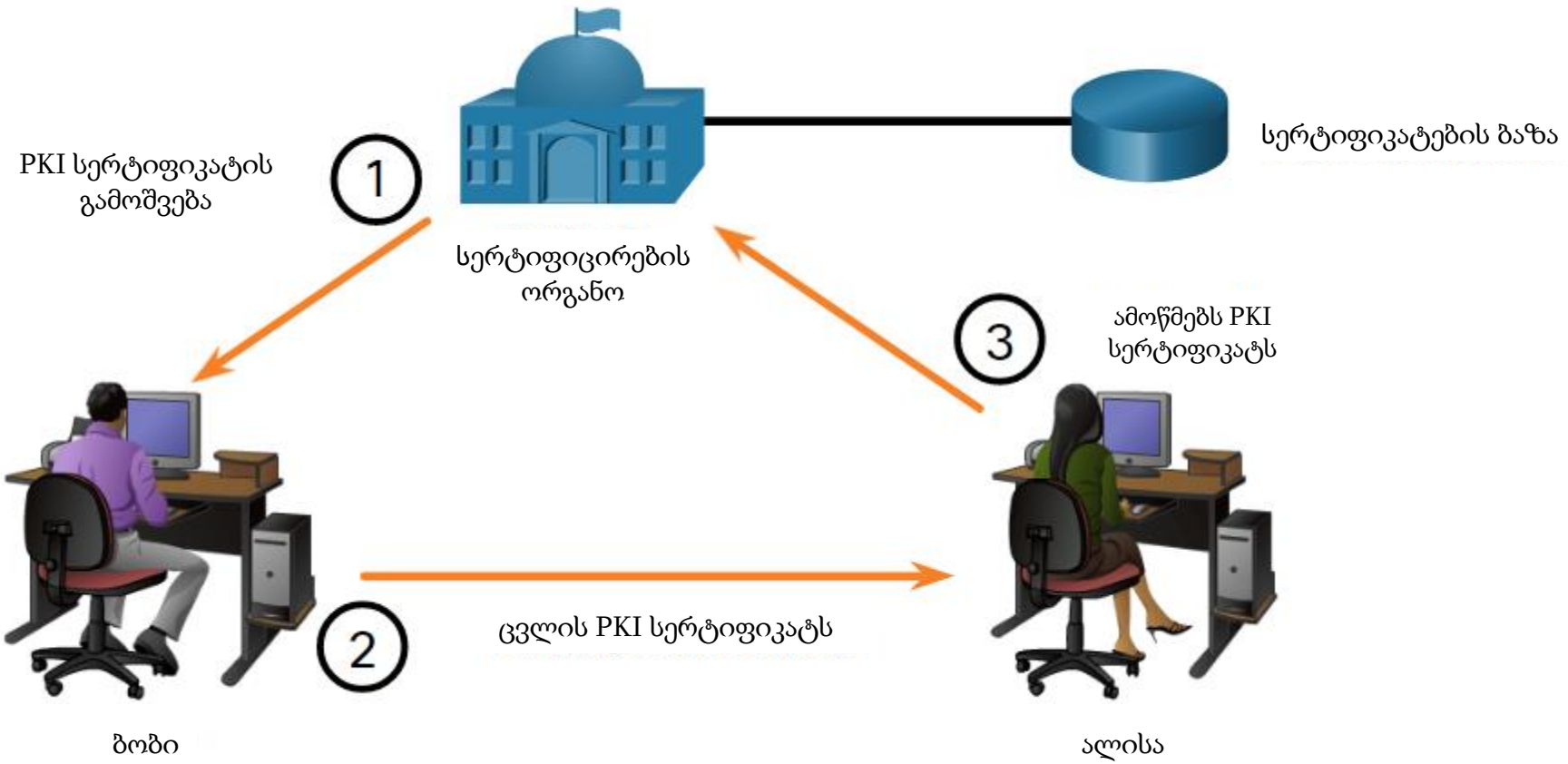
ალისა ცდილობს ჩეკით გადახდას.

ალისას ვინაობა დადასტურებულია მისი მართვის მოწმობის შემოწმების შემდეგ

PKI-ს სტრუქტურა - PKI სტრუქტურის ელემენტები



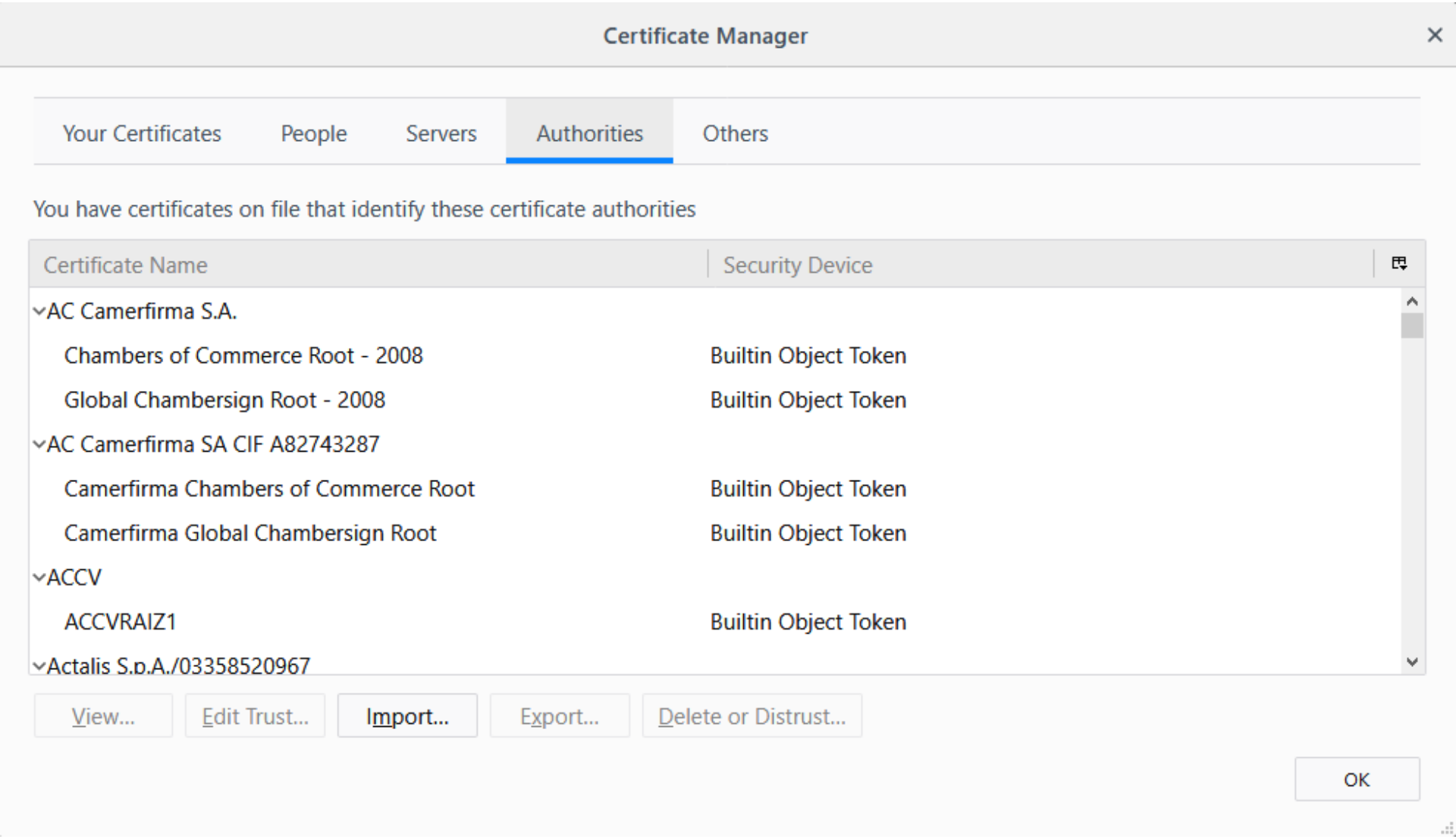
PKI-ს სტრუქტურა - PKI-ს მაგალითი



სერტიფიცირების ორგანოები - სერტიფიკატების კლასები

კლასი	აღწერა
0	გამოიყენება ტესტირებისთვის, რომლითაც არავითარი შემოწმება არ სრულდება
1	გამოიყენება ფიზიკური პირისთვის, ელექტრონული ფოსტის შემოწმების მიზნით
2	გამოიყენება ორგანიზაციებისთვის, რომლებიც საჭიროებენ ნამდვილობის შემოწმებას
3	გამოიყენება სერვერებისა და პროგრამული უზრუნველყოფის ხელმოწერისთვის, რომელთათვისაც სრულდება ვინაობისა და უფლებამოსილების დადასტურება და შემოწმება, სერტიფიცირების ორგანოს მიერ
4	გამოიყენება კომპანიებს შორის ბიზნეს ტრანზაქციებისთვის ონლაინ რეჟიმში
5	გამოიყენება კერძო კომპანიების ან სამთავრობო უსაფრთხოებისთვის

სერტიფიცირების ორგანოები - VeriSign სერტიფიკატების ნიმუში

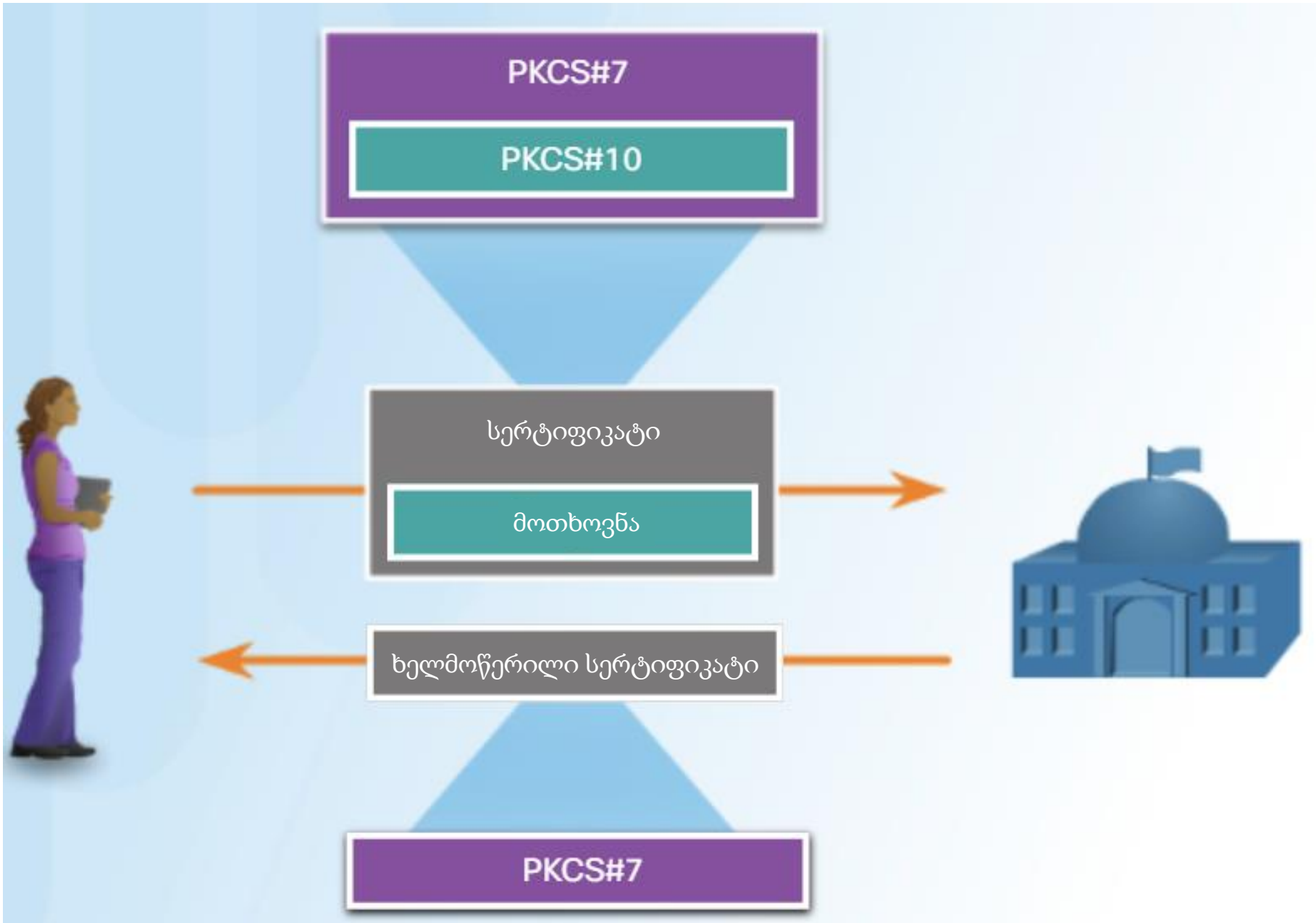


ღია-გასაღებით კრიპტოგრაფიის სტანდარტები - RSA PKCS სტანდარტები

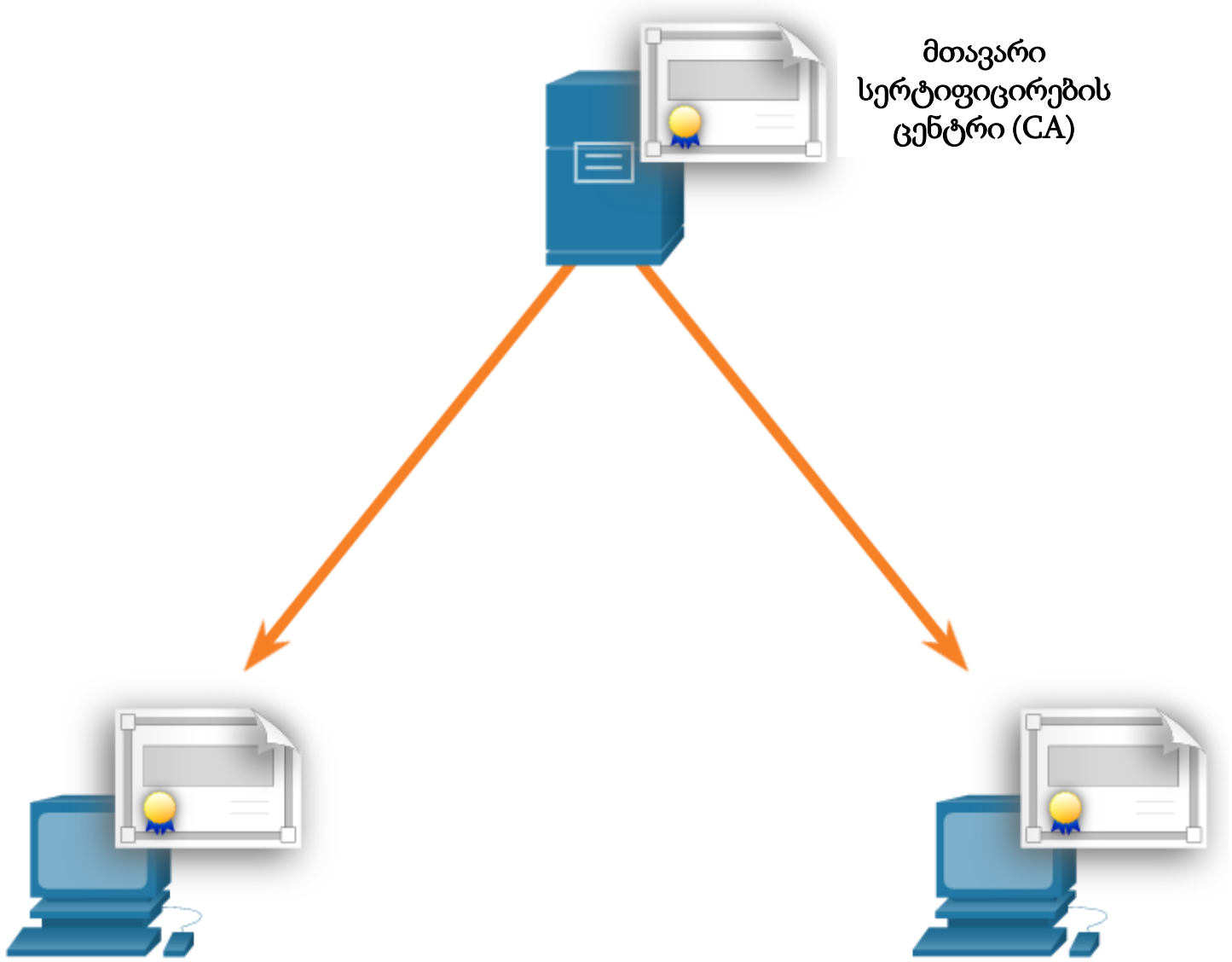
RSA PKCS სტანდარტები

- PKCS #1: RSA კრიპტოგრაფიული სტანდარტი
- PKCS #3: DH გასაღებების შეთანხმების სტანდარტი
- PKCS #5: პაროლზე დაფუძნებული კრიპტოგრაფიული სტანდარტი
- PKCS #6: გაფართოებული სერტიფიკატის სინტაქსის სტანდარტი
- PKCS #7: კრიპტოგრაფიული შეტყობინების სინტაქსის სტანდარტი
- PKCS #8: დახურული გასაღების ინფორმაციის სინტაქსის სტანდარტი
- PKCS #10: სერტიფიცირების მოთხოვნის სინტაქსის სტანდარტი
- PKCS #12: პერსონალური ინფორმაციის გაცვლის სინტაქსის სტანდარტი
- PKCS #13: ელიფსური მრუდის (Elliptic Curve) კრიპტოგრაფიული სტანდარტი
- PKCS #15: კრიპტოგრაფიული ტოკენის ინფორმაციის ფორმატის სტანდარტი

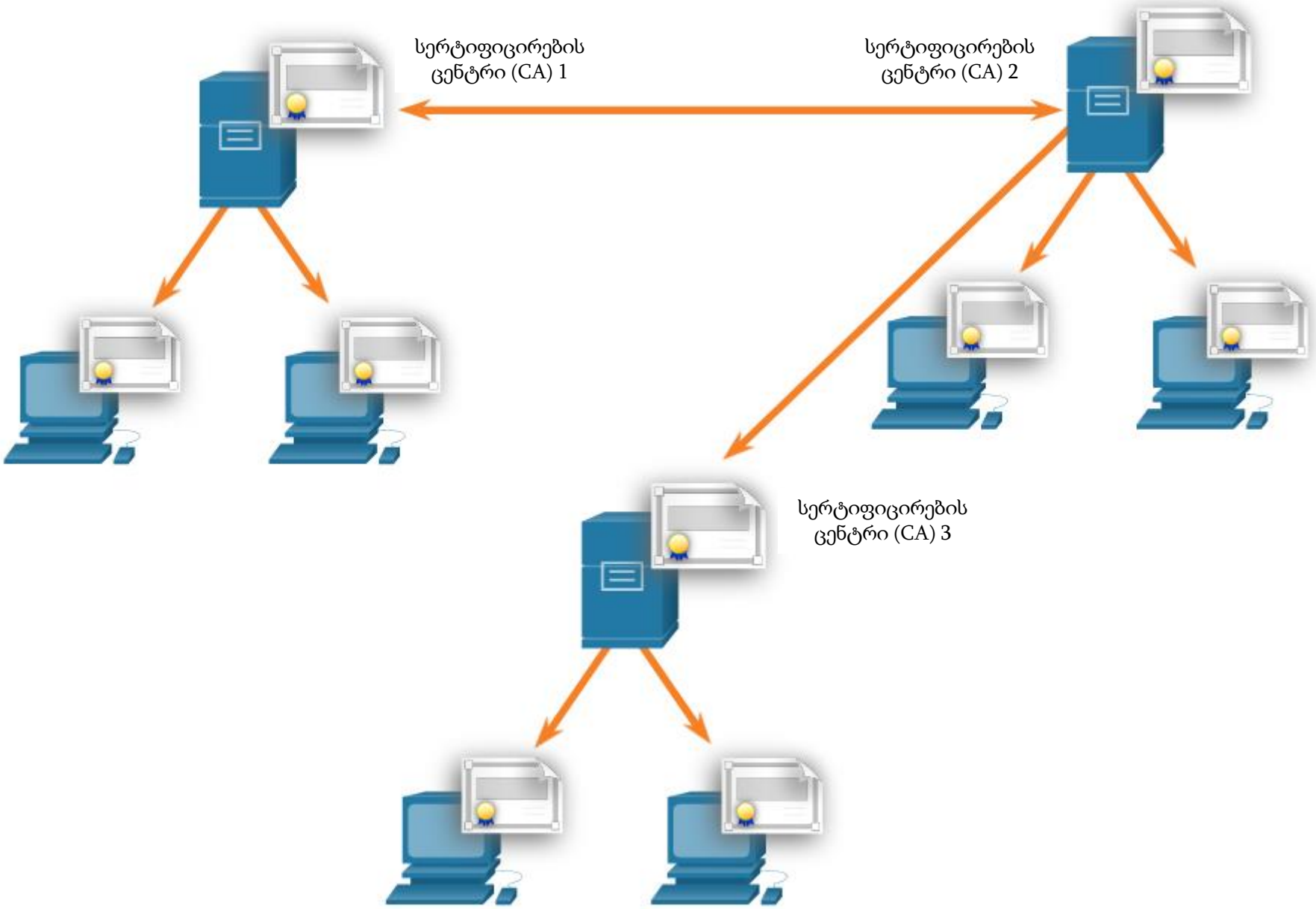
სერტიფიკატების რეგისტრაციის მარტივი პროტოკოლი - PKCS-ის მაგალითი



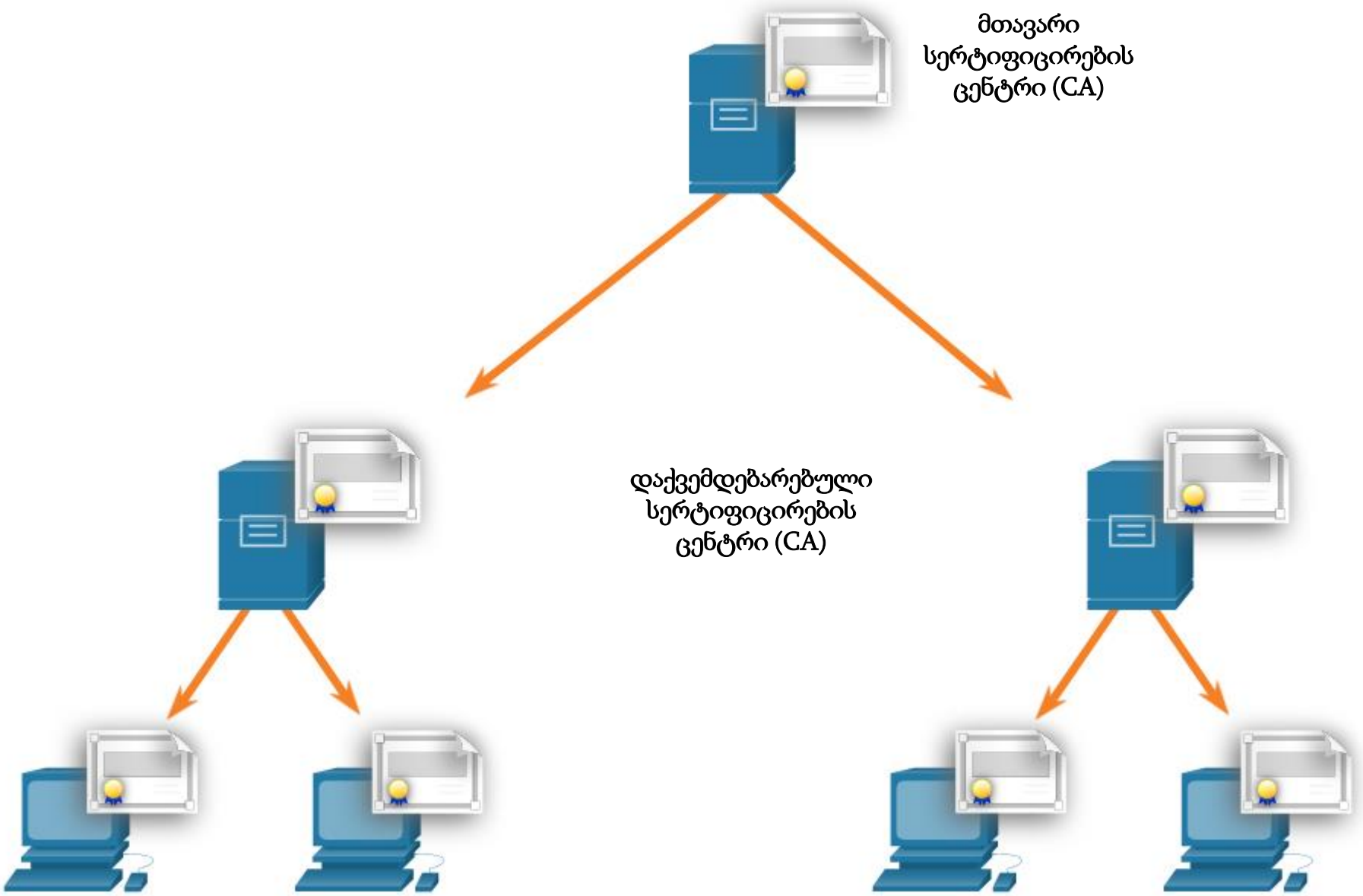
PKI ტოპოლოგიები - ერთ ძირის მქონე (single-root) PKI ტოპოლოგია



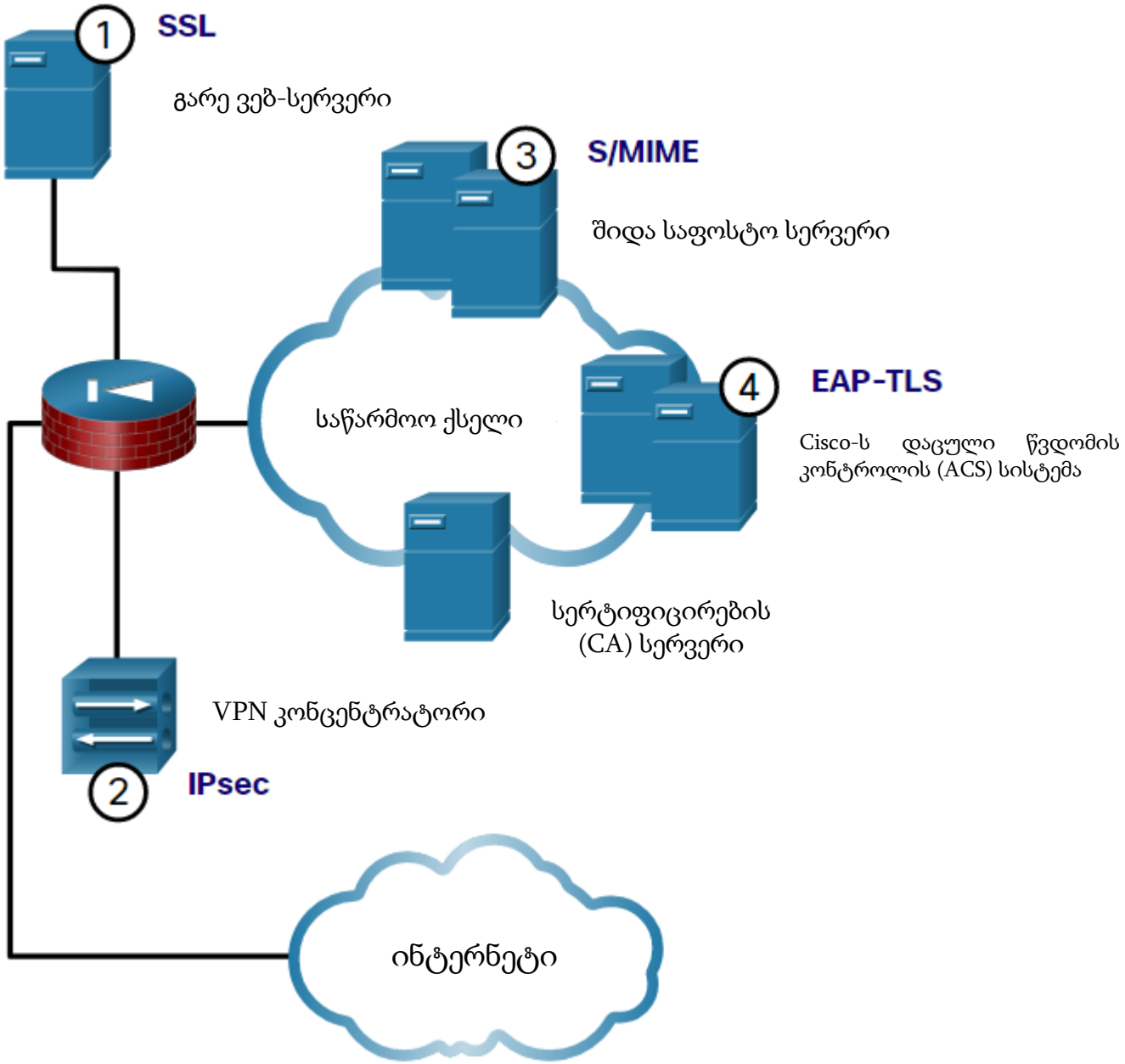
PKI ტოპოლოგიები - ჯვარედინი სერტიფიცირების CA



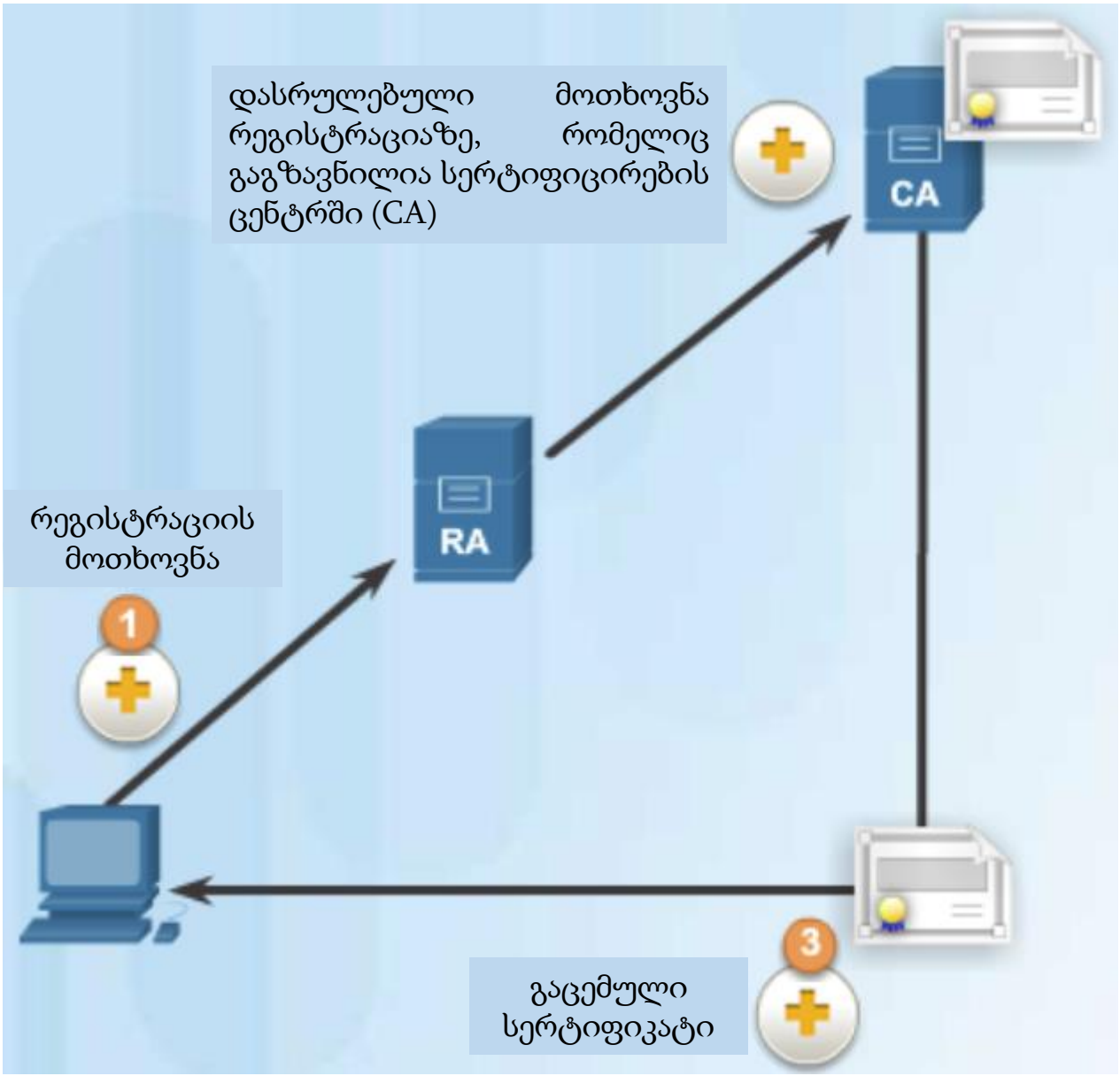
PKI ტოპოლოგიები - იერარქიული CA



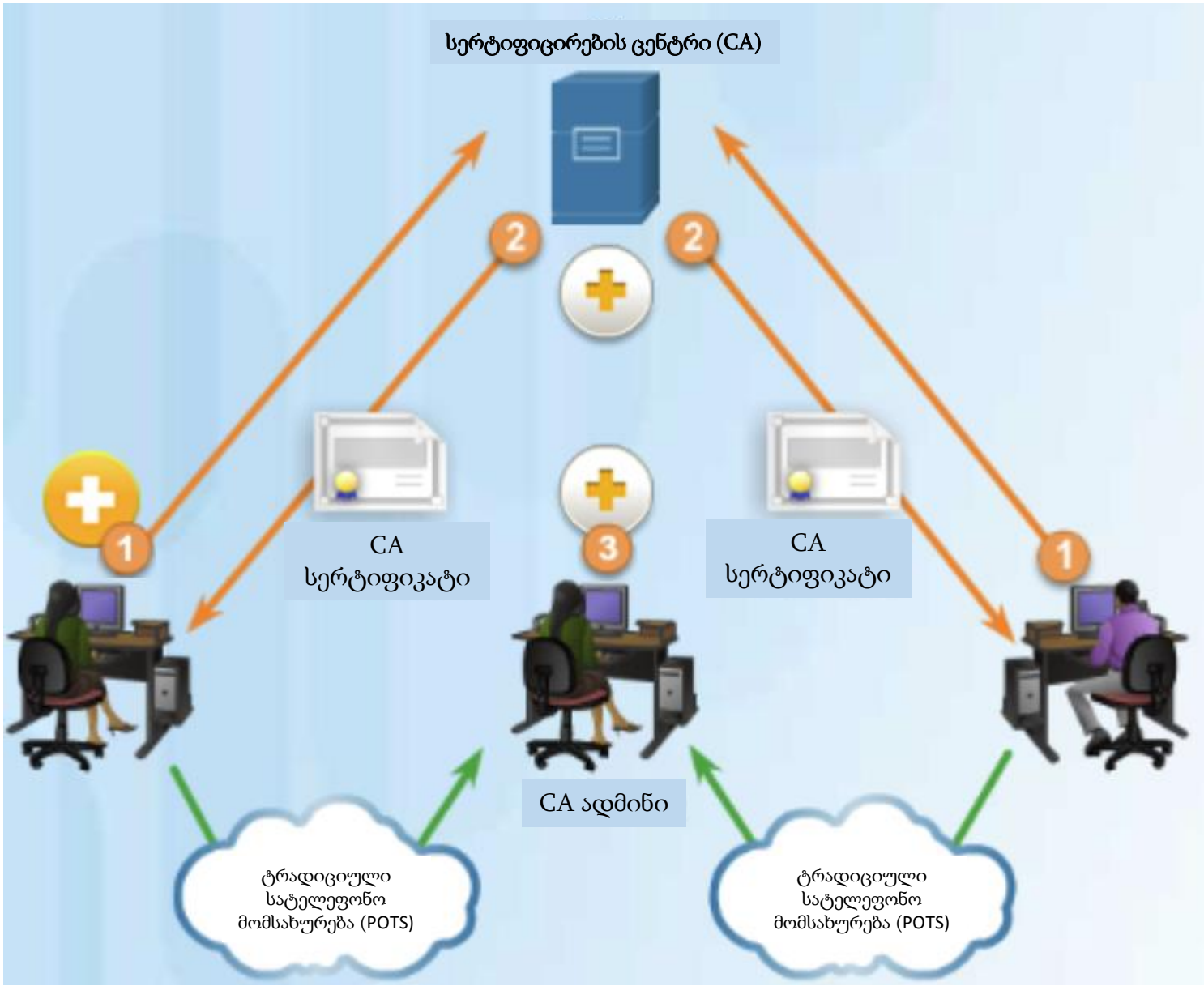
სხვადასხვა PKI მწარმოებლების თავსებადობა - X.509v3 აპლიკაციები



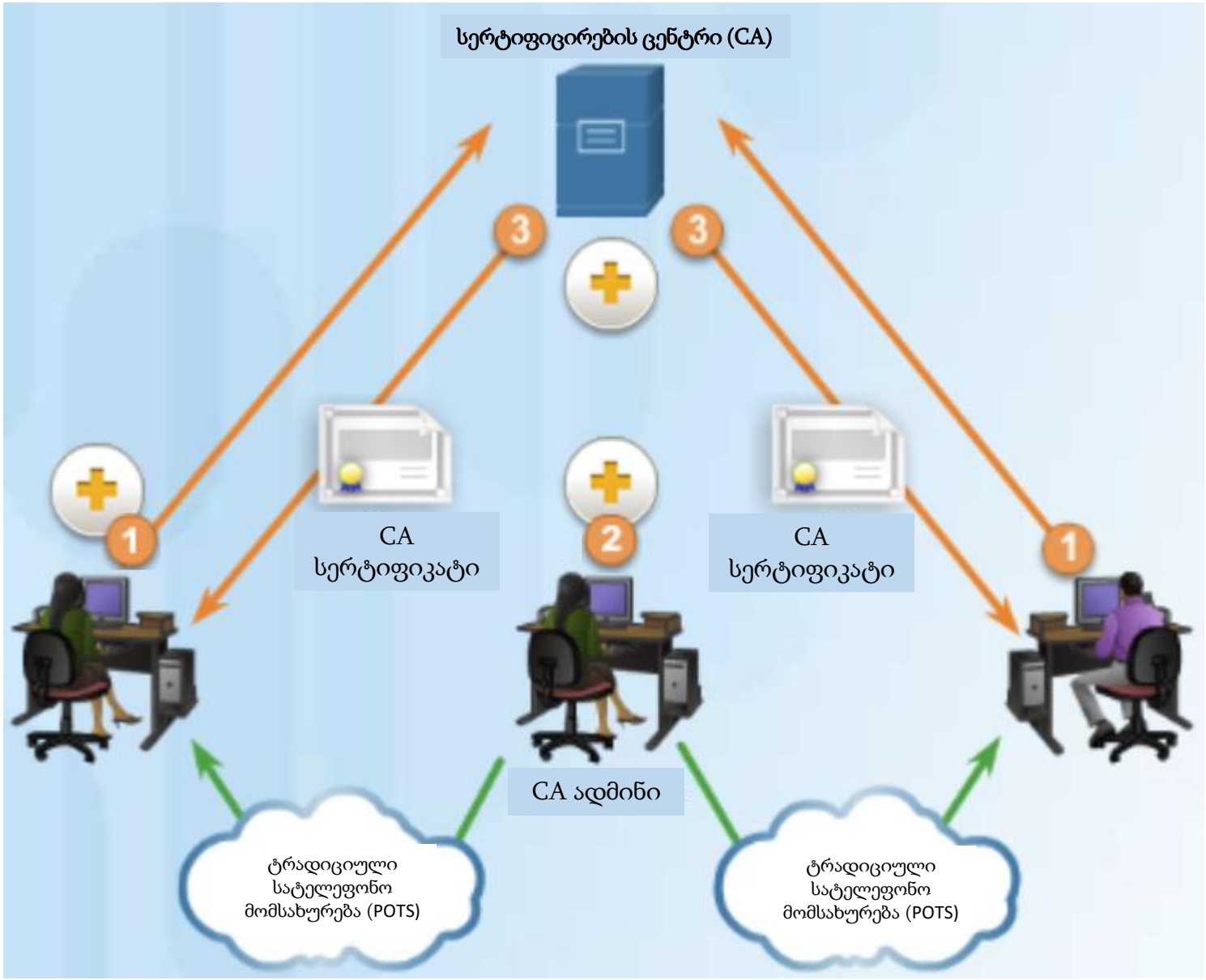
მარეგისტრირებელი ორგანო - მარეგისტრირებელი ორგანოები



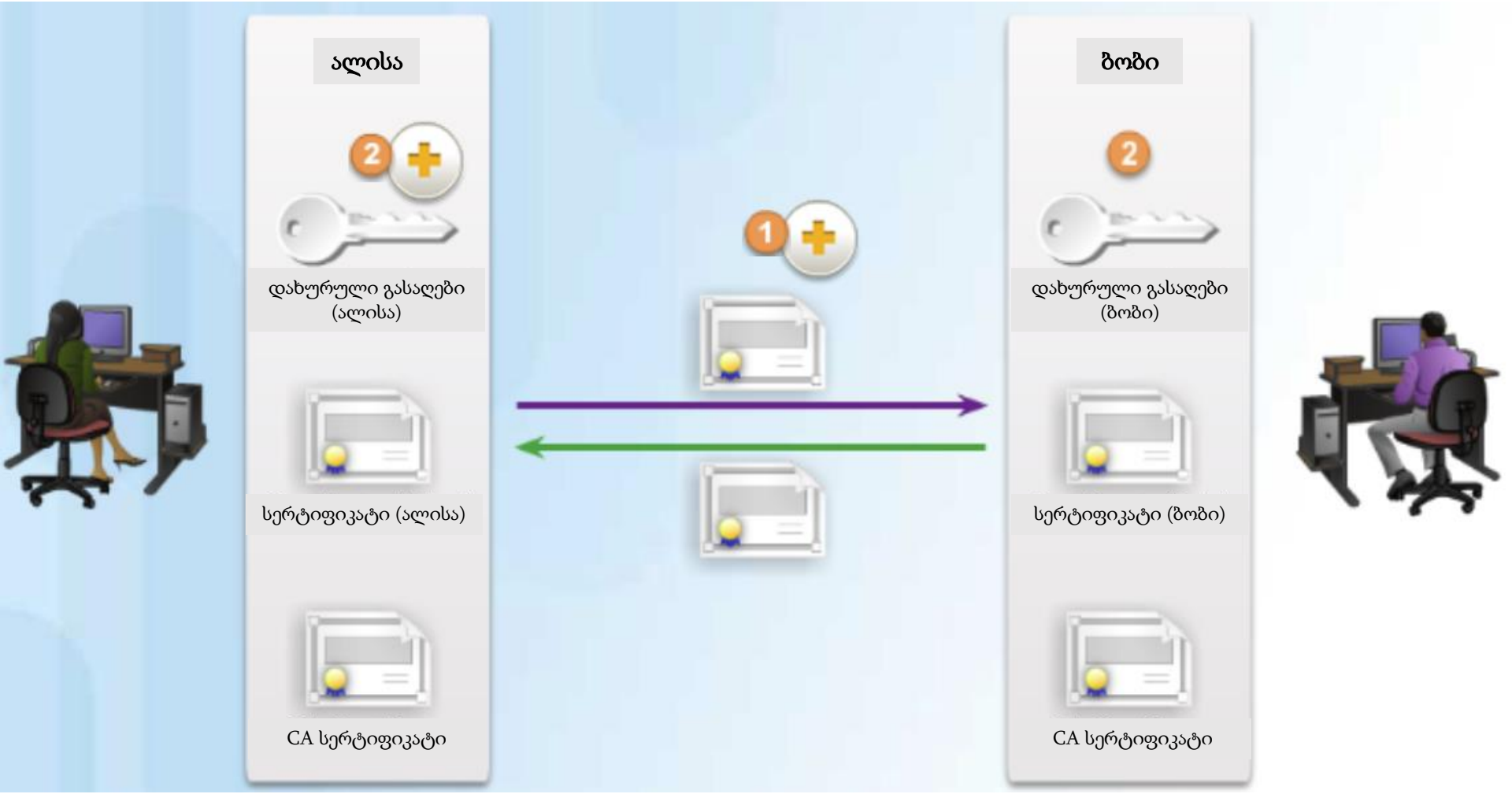
ციფრული სერტიფიკატები და სერტიფიცირების ორგანოები (CA) – CA სერტიფიკატების მიღება



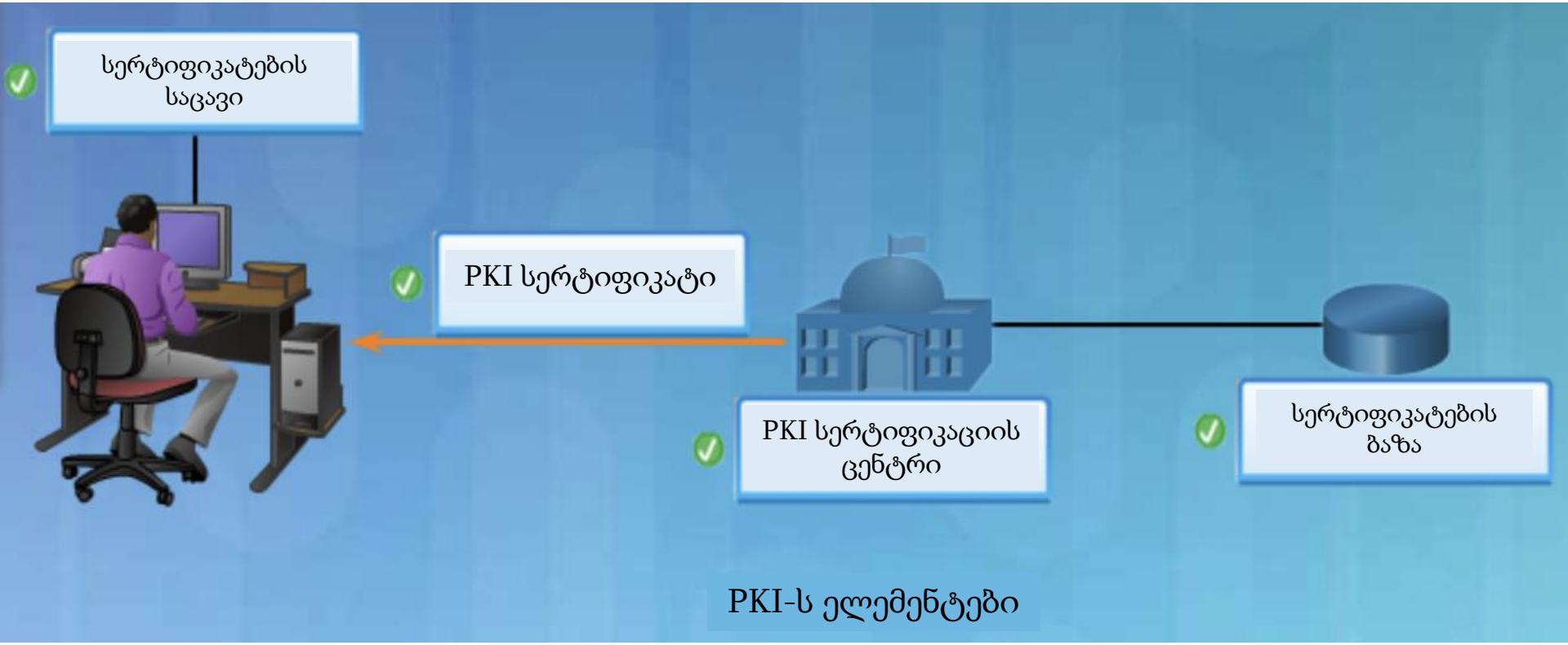
ციფრული სერტიფიკატები და სერტიფიცირების ორგანოები (CA) - სერტიფიკატის მოთხოვნების გადაცემა სერტიფიცირების ორგანოსთან (CA)



ციფრული სერტიფიკატები და სერტიფიცირების ორგანოები (CA) - კვანძები ახდენენ აუთენტიკაციას ერთმანეთთან



აქტივობა - PKI სტრუქტურის ელემენტების იდენტიფიკაცია



PKI-ს ელემენტები

გმადლობთ ყურადღებისათვის!!!