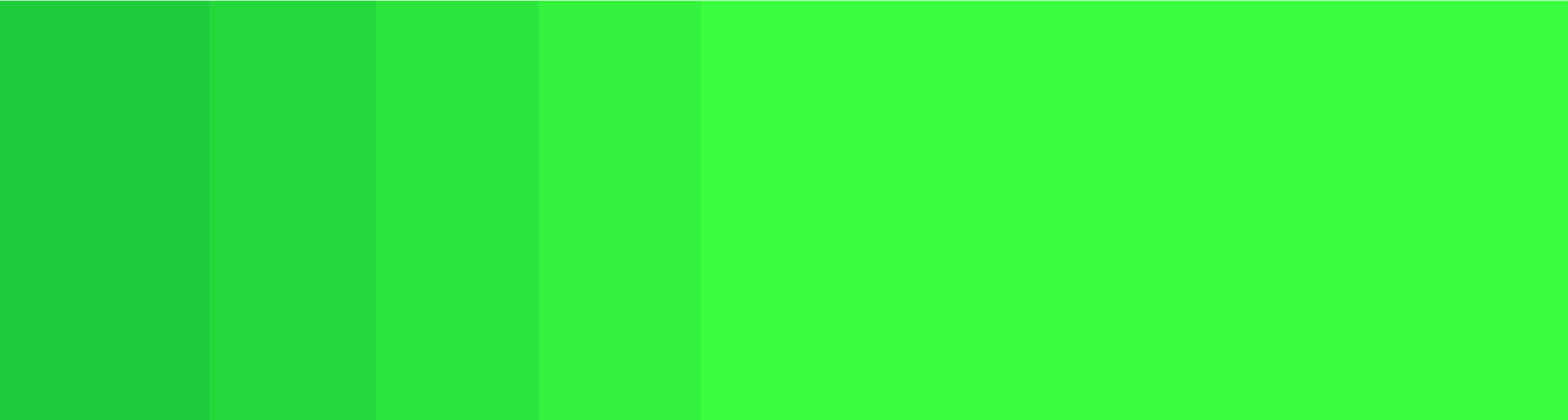


PKI Giriş



Sapagyň tertibi

- Asimmetrik kriptografiya
- PKI guramasy
- HSM
- TSA

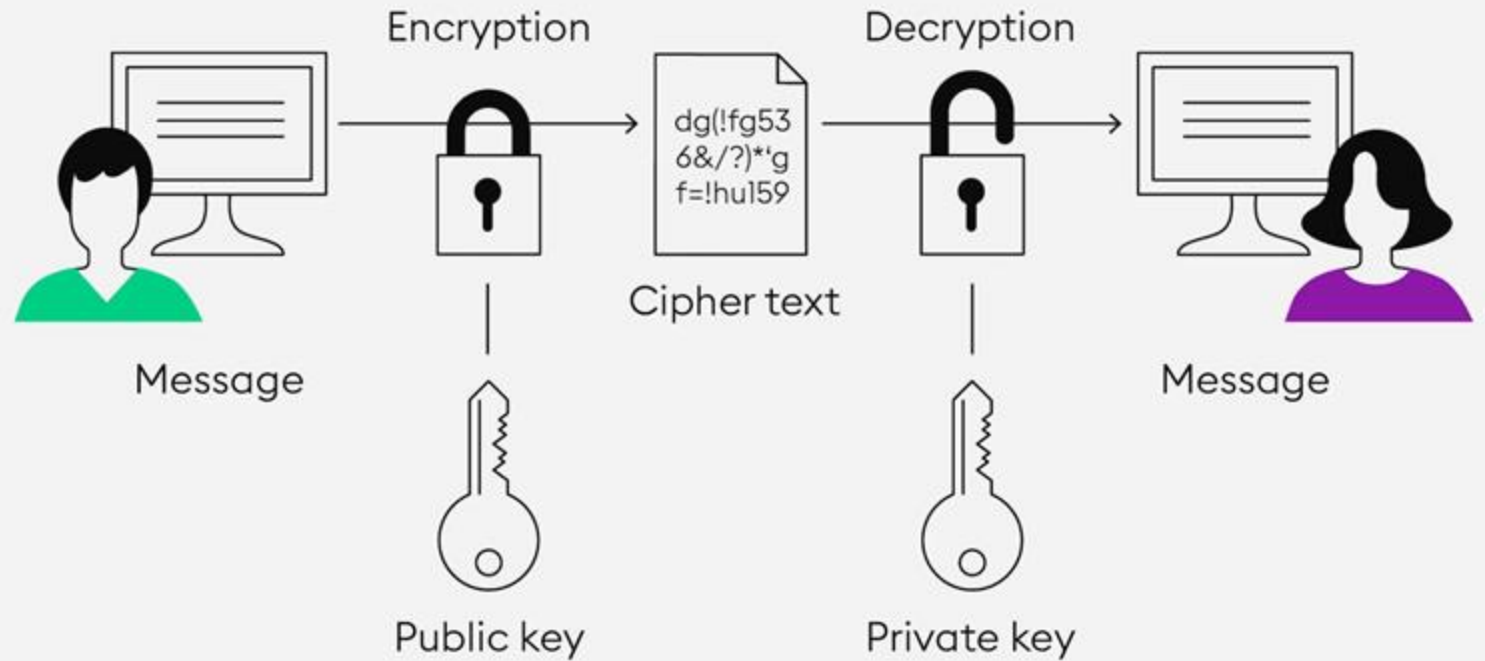
Asimmetrik kriptografiya



Asimetrik açar döretmek

Bir tema üçin hemişe bir jübüt açar

ASYMMETRIC ENCRYPTION

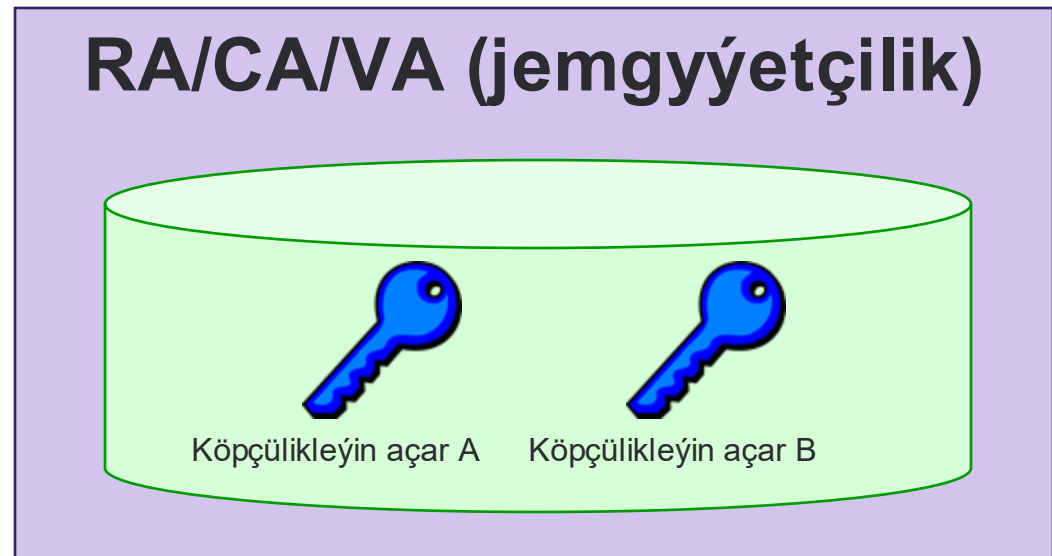


Surat <https://bitpanda-academy.imgix.net/450037a5-144d-44ef-9db1-7fe7ce1f433d/bitpanda-academy-expert-20-what-is-asymmetric-encryption-infographic.png?auto=compress%2Cformat&fit=min&fm=jpg&q=80&w=2100> sahypasyndan alyndy.

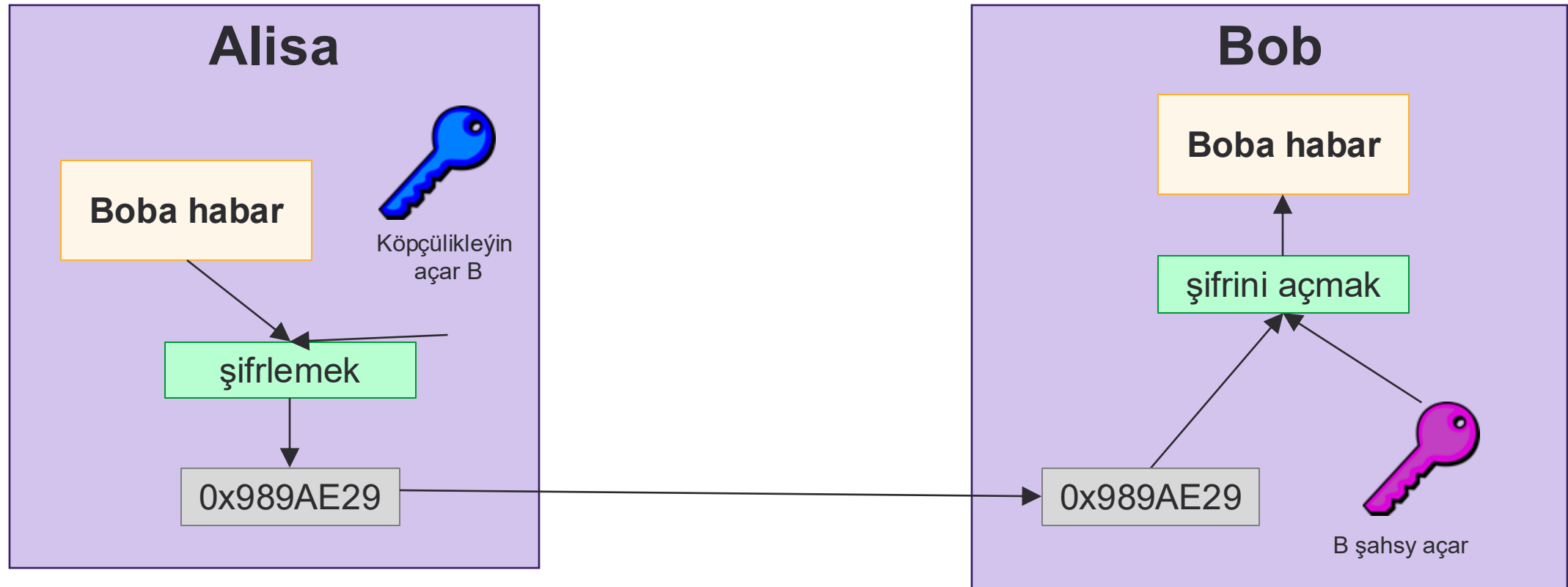
Sertifikatlar

Sertifikatlar açarlary temalara baglaýar

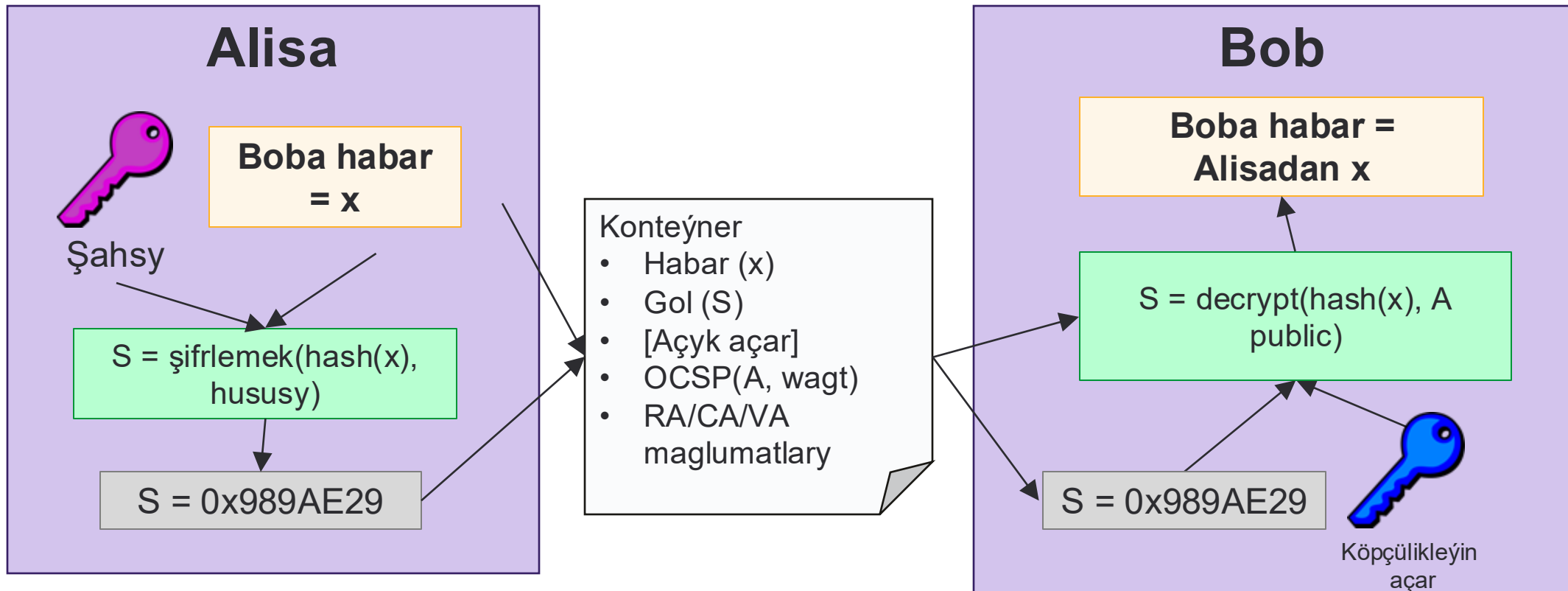
- **Bellige alyş edarasy (RA)**
subýektiň hakykylygyny kepillendirýär.
- **Sertifikatlaşdyryş edarasy (CA)**
Sertifikat döredýär – açyk açaryň subýektiň şahsyýetine baglanýandygynyň sanly gol çekilen tassyklamasy.
- **Tassyklaýyş edarasy (VA)**
Sertifikat baradaky maglumatyň ygtybarlydygyny we elýeterlidigini üpjün edýär.
- Okaň: Eýesi gizlin açaryň gözegçiliginde.



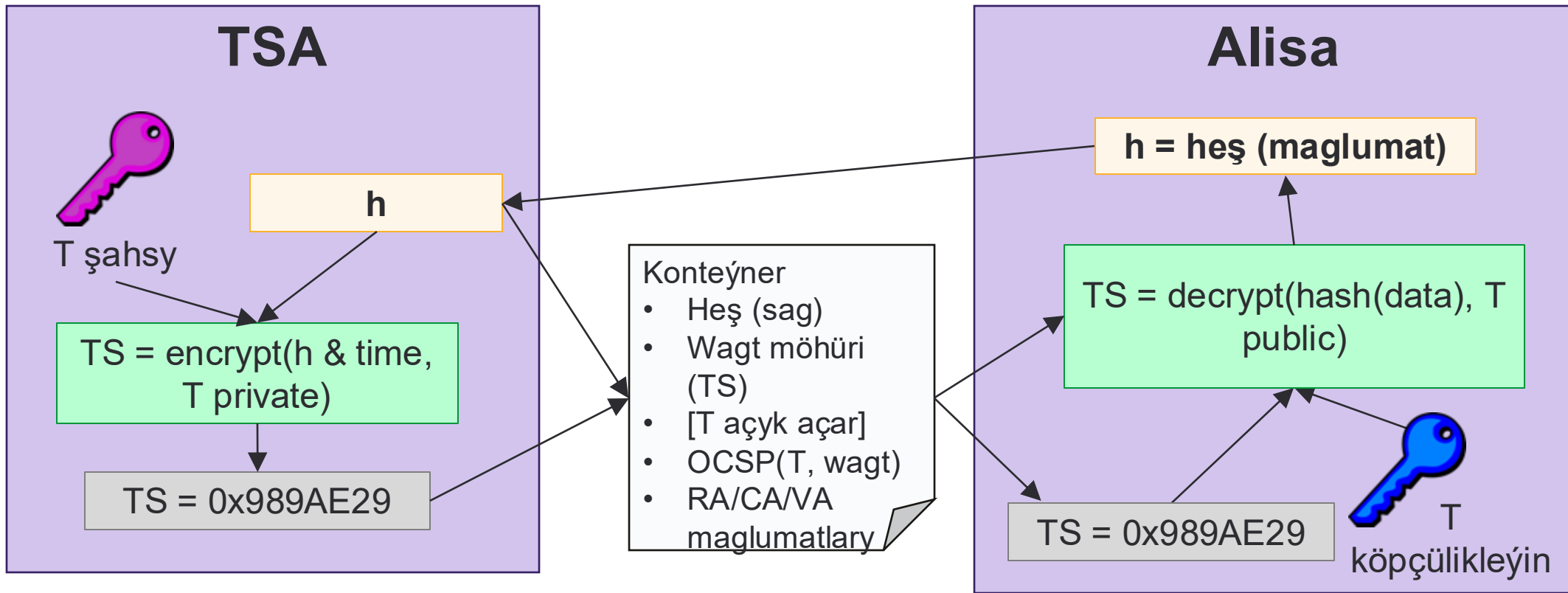
Şifrlmek – diňe Bob asyl habary okap biler



Gol çekmek – Bob munuñ Alisadan bolandygyna ynanyp biler



Wagt möhürleme – Alisa belli bir wagtda käbir maglumatlaryň bardygy barada subutnama döredýär



Asimmetrik kriptografiýa diňe şeýle ýagdaýda işleýär...

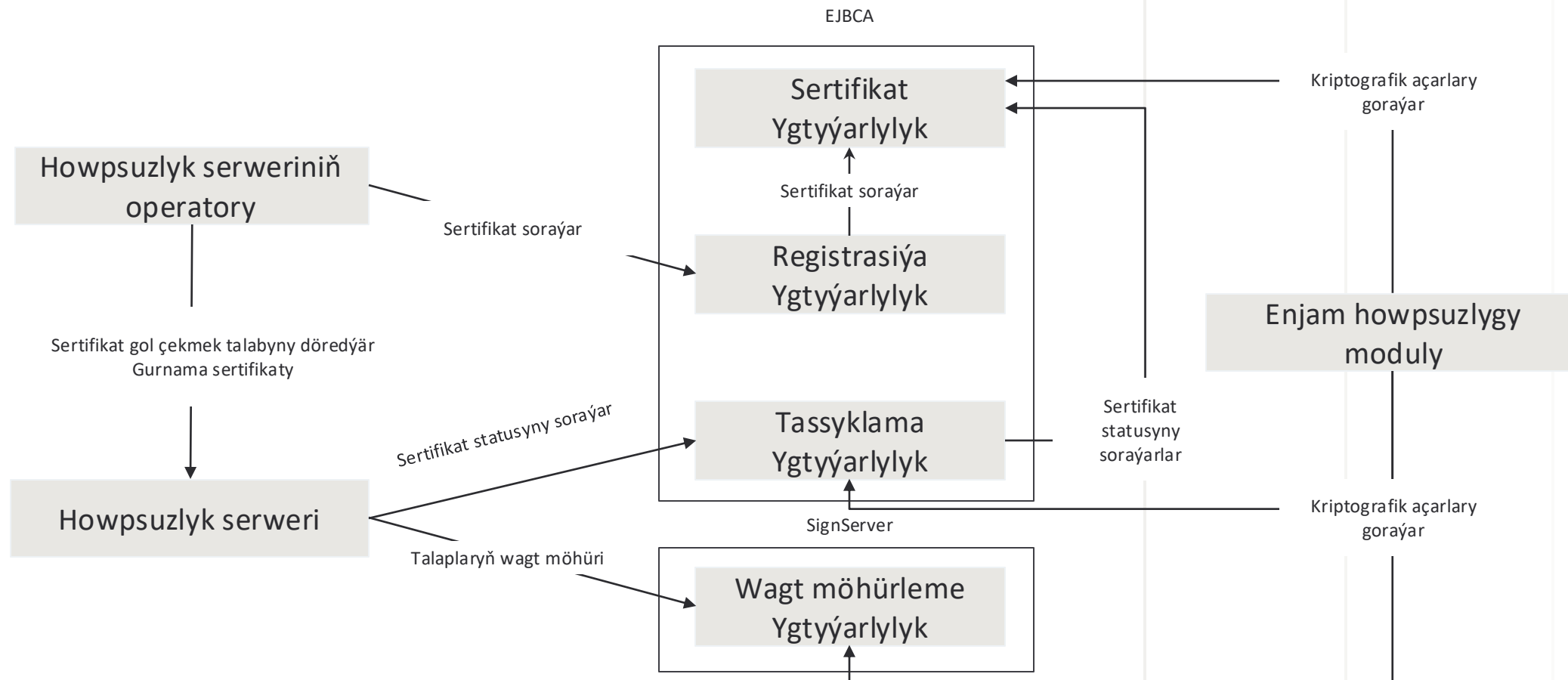
- Şahsy açar gizlin saklanýar - ýokary gizlinlik.
 - HSM, SSCD, QSCD we ş.m.
 - PIN siziň şahsy açaryňyz däl.
- Açyk açar elýeterlidir - ýokary bitewilik we elýeterlilik.
 - RA/CA/VA auditleri we ätiýaçlandyryş.
- Matematika dogry ornaşdyrylan.
 - 2017-nji ýylda ROCA-gowşaklygy!
 - <https://arstechnica.com/information-technology/2017/10/crippling-crypto-weakness-opens-million-of-smartcards-to-cloning/>

Açık açar infrastrukturasy

Asimmetrik kriptografiýany ýerine ýetirýän tehnologiýa we gurama



PKI-a umumy syn





Sertifikat beriş ygtyýarlygy

- Iki gatly arhitektura
 - Kök
 - Orta derejeli
- Sertifikatlary berýär
- Sertifikatlara gol çekýär
 - Bu gol sertifikatyň hakykydygyna we CA-ny kanuny diýip ykrar edýän islendik adam tarapyndan ynamdardygyna kepil geçýär
- Sertifikatyň ýatyrylmagynyň sanawyny (CRL) we sertifikatyň statuslaryny (OCSP maglumat bazasyny) berýär

Enjam Howpsuzlyk Moduly (HSM)

- Kriptografik açarlary goramak üçin niýetlenen enjam
 - Açarlar işjeňleşdirilende klientden HSM-e ýüklenýär
 - Dynç alnan açarlar klientde binar obýektler hökmünde ýerleşýär (/opt/nfast/kmdata)
- Bozulmaga garşy sertifikatlaşdyrylan enjam
 - Gizlinlik barada duýduryşlar
 - Enjamy diňe öndüriji açmaga rugsat berýär! Bolmasa, ynam ýitirilýär.
- Ynam üpjün edýär



Apparat Howpsuzlygy Moduly (HSM) - kart toplumlary

- K/N syýasaty
- Dürli işler üçin açarlar (akylly kartlar)
 - Administrator kart toplumy (ACS) enjam dolandyryşy üçin niýetlenendir
 - Başlangyçlaşdyрма
 - Dikeltmek
 - Gaýtadan ulanyp bolmaýar!
 - Operator kart toplumy (OCS) kriptografik açarlary goraýar
 - HSM-de gitme!
 - CA we TSA-ny işjeňleşdirmekde (başlatmakda we täzeden başlatmakda) ulanylýar
 - Fiziki taýdan bar bolmak zerurdyr
 - Formatlaşdyryp we gaýtadan ulanyp bolýar
- Kartlar howpsuz ýerde saklanmaly!



HSM - gurnamaga taýýarlyk

- Uzakdaky faýl ulgamy (RFS)
 - HSM konfigurasiýasyny saklaýar
- Kart toplumlary
 - K/N meseleleri
- Syýasatlar
 - Enjamy kim dolandyrmaga rugsat berilýär
 - Ähli işler hasaba alynmaly

HSM - başlangyç konfigurasiýa

- RFS taýýar bolmaly
- Ilkinji enjam bilen täze howpsuzlyk dünýäsi döredilýär
- Indiki enjamlar bar bolan howpsuzlyk dünýäsini ýükleýär
- Klientler (IP adresleri) goşulmaly
 - Soňra hem goşup bolýar



HSM - ätiýaçlyk

1. RFS-de /opt/nfast-yň ätiýaçlyk nusgasyny saklaň
2. Ähli klientlerde /opt/nfast-yň ätiýaçlyk nusgasyny saklaň
3. Kart toplumlarynyň nusgalaryny ätiýaçlyk üçin döredip bolýar
 - a. Howpsuz ýerde saklanmaly!

HSM - dikeltmek

1. RFS-de klient programma üpjünçiligini gurnaň
2. RFS-iň /opt/nfast/kmda-ny dikelt
3. HSM-i konfigurirläň we bar bolan howpsuzlyk dünýäsini ýükleň
 - a. ACS ygtyýarlandyrmak üçin gerek
4. Klient programma üpjünçiligini klientlere gurnaň
5. Klientlerde /opt/nfast/kmda dikelt



HSM - tehnik hyzmat

- Programma üpjünçiliginiň täzelenmeleri
 - Öndüriji tarapyndan üpjün edildi
- Howpsuzlyk dünýäsi programma üpjünçiliginiň täzelenmeleri
 - Öndüriji tarapyndan üpjün edildi
- Müşderiler hem täzelenmeli



HSM - esasy prosesler

- HSM-i dikeltmek üçin ACS gerek
- CA we SingServer işe girizmek üçin OCS gerek

HSM - maslahat we garaýyşlar

- nfkminfo çykyşynyň töwereginde gözegçilik skriptlerini dörediň
- Daşky gurşawy synagdan geçirmek üçin azyndan 1 enjam satyn alyň
- HA üçin önümçilik üçin goşmaça enjamlary satyn alyň
- Ähli zady uzakdan dolandyrmak üçin uzakdan işleýän operator funksiýasyny satyn alyň
 - ACS/OCS bilen operasiýalary goşmak bilen
- Günlük ýygnaýjy bilen gündelikleri ýygnaň we olary gündelik serwerinde saklaň

EJBCA ulanýan bellige alyş edarasy (RA)

- EJBCA-nyň bir bölegi
- Çykarmak üçin RA web
- Ýatymak EJBCA admin web sahypasynda amala aşyrylýar

SignServer
ulanyp,
wagt
möhürleme
ygtyýarlygy
(TSA)





TSA - gurnamaga taýýarlyk

TSA - Ilkinji konfigurasiya

- Ansible oýun kitaby bilen ýerleşdirildi
- Docker konteýner
 - Java dilinde ýazylan we wildfly-da işleýär
 - Kubernetes üçin helm diagrammasy elýeterlidir
- Autentifikasiya üçin Management CA (EJBICA-dan)
 - Şeýle hem, EJBICA-dan öz aýratyn CA-sy bolup biler



TSA - ätiýaçlyk nusga we dikeltmek

- Ätiýaçlyk
 - PostgreSQL maglumat bazasy
 - PostgreSQL surat esasyndaky ätiýaçlyk nusgalaryny döredende ätiýaçlyk nusgasyny göçürip almak režimine geçirilmelidir
 - Konteýnerler döwletsiz, ätiýaçlyk nusgasyny göçürmegiň zerurlygy ýok
- Dikeltmek
 - Maglumat bazasyny dikeltmek
 - Konteýnerleri mümkin bolan oýun kitaby bilen ýerleşdiriň
- Saýtyň bökdençsiz işlemegini dikeltmek üçin alternatiwa hökmünde göz önünde tutmaly
 - Repmgr replikasiýany dolandyrmak üçin ulanylýar



TSA - tehnikai hyzmat

- TSA sertifikatynyň ornuny tutmak
- Programma üpjünçiligini täzelemek
 - Oýun kitapçasyndaky wersiýany üýtget
 - Oýun kitabyňy ulanyň



TSA - maslahatlar we garaýyşlar

- tsget/openssl bilen monitor
 - TKM repozitoriýasyndaky pki/tests katalogyna serediň
- Synag gurşawyny HA režiminde ýerleşdiriň
 - Synag önümçilik hökmünde kabul edilmelidir
- Içki synag üçin işläp düzmek gurşawyny dörediň
- Synag gurşawy üçin HSM-leri satyn alyň
- Günlük ýygnaýjy bilen gündelikleri ýygnaň we olary gündelik serwerinde saklaň