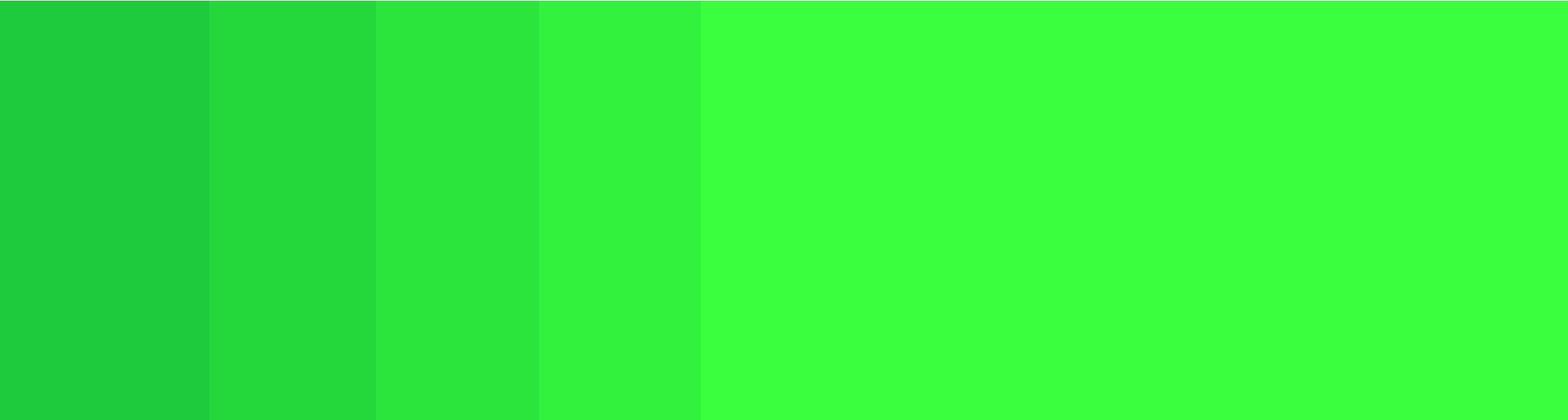


Trust Hyzmat Infrastrukturas



Sapagyň tertibi

Tema	Çaklanylýan wagt
Giriş we açylyş	14.30
Teoriýanyň gysgaça mazmuny	14.45
CA tejribesi	15.15
Arakesme	16.20
CA tejribesi dowam edýär	16.40
Wagt möhürlemek tejribesi	17.15
Sorag-jogap	18.00
Synag	18.15

Tassyklaýyş ygtyýarlygy

- Onlaýn sertifikat statusy protokoly (OCSP)
 - Sertifikat güýjündemi?
 - X-Road tarapyndan ulanylýar
 - CRL köneldi
- Sertifikat statusy CA maglumat bazasyndan soralýar
- Aýratyn programma nusgasy hökmünde konfigurirlenip bilner



Bellige alyş edarasy

- Ulanyjynyň kimligini tassyklaýar
- Sertifikat talaplaryny tassyklaýar
- Sertifikat ömrüniň siklini dolandyýar
 - CA-dan sertifikat soraň
- Aýratyn programma nusgasy hökmünde konfigurirlenip bilner



Wagt möhüri goýýan ygtyýarly edara

- Howpsuzlyk serweriniň habar žurnaly üçin sanly wagt möhürini üpjün edýär
 - Wagt möhüri sertifikaty ýörite aralyk CA-dan berildi
- Kriptografik açarlar HSM tarapyndan goralýar



Sertifikat bermegiň prosesi

1. Sertifikat gol çekmek talaplary (CSR) howpsuzlyk serwerinde ulgam administratory tarapyndan döredilýär
2. Sistem administratory KSM-i bellige alyş edarasyna (RA) iberýär
3. RA KSM-leri tassyklaýar
4. RA KSS-leri sertifikatlaşdyryş edarasyna (CA) iberýär
5. CA KSM-lere (berilen güwänama) gol çekýär
6. CA operatory howpsuzlyk serwer operatoryna sertifikat iberýär





Sertifikatyň ýatyrylmagy prosesi

1. Sertifikatyň ýatyrylmagy prosesi dürli sebäplere görä başlanýar
 - Howpsuzlyk serweri işini bes edýär
 - Howpsuzlyk serweriniň hususy açary howp astyna düşdi
 - Howpsuzlyk serweri indi ulanylmaýar
2. Sertifikaty ýatyrmaq zerurlygy barada CA operatoryna habar berilýär
 - CA operatory CA maglumat bazasyndaky sertifikaty ýatyrýar
 - VA sertifikat statusy baradaky haýyşnama boýunça ýatrylan status bilen (sebäbini görkezip) jogap bermäge başlaýar
3. CA täze CRL döredýär

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 açmaga diňe öndüriji 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
 - Ony soňrak hem goşup bolýar



HSM - ätiýaçlyk

1. RFS-de
2. Ähli klientlerde
3. Kart toplumlarynyň nusgalaryny ätiýaçlyk üçin döredip bolýar
 - a. Howpsuz ýerde saklanmaly!

HSM - dikeltmek

1. RFS-de klient programma üpjünçiligini gurnaň
2. RFS-iň
3. HSM-i konfigurirläň we bar bolan howpsuzlyk dünýäsini ýükleň
 - a. ygtyýarlandyrmak
4. Klient programma üpjünçiligini klientlere gurnaň
5. Klientlerde

A close-up photograph of a person's hands cleaning a white, reflective surface, likely a desk or table, with a white paper towel. The background is blurred, showing other people in a meeting or office setting.

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
- SingServer işe girizmek

HSM - maslahat we garaýyşlar

- nfkminfo çykyşynyň
- Daşky gurşawy barlamak 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





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, şonuň üçin ätiýaçlyk nusgalaryny göçürmegiň zerurlygy ýok
- Dikeltmek
 - Maglumat bazasyny dikeltmek
 - Ansible oýun kitaby bilen konteýnerleri ýerleşdiriň
- Saýtyň bökdençsiz işlemegini dikeltmek üçin alternatiwa hökmünde göz öňünde tutmaly
 - Repmgr replikasiýany dolandyrmak üçin ulanylýar



TSA - tehnikai hyzmat

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



TSA - maslahatlar we garaýyşlar

- tsget / openssl
 - TKM repozitoriýasyndaky
- Synag gurşawyny HA režiminde ýerleşdiriň
 - Synaglar 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

Okuw gurşawy

- Her bir stažýoryň öz wirtual maşyny bar
 - training.ca{1-5}.pki.gov.tm
- Uç nokatlary
 - training.ca{1-5}.pki.gov.tm - AIA, CRL, EJBCA admin web sahypasy
 - tälim.ocsp{1-5}.pki.gov.tm - OCSP
 - training.tsa{1-5}.pki.gov.tm - Wagt möhürleme hyzmaty, SignServer admin web
- SSH güwänamalary
 - Ulanyjy ady: pki
 - Parol: XroadPKI123!

EJBCA we TSA-ny ornaşdyrmak

1. SSH-den VM-e:

```
ssh pki@training.ca1.pki.gov.tm
```

1. ansible we git- lfs gurnaň :

```
sudo apt gurnamak üçin git- lfs
```

1. Klon ammary:

```
git klony https://gitlab.xroad.gov.tm/roksnet/tkm.git
```

1. Katalogy üýtgetmek:

```
cd tkm / pki /ansible
```

1. Mümkin rollary gurnaň:

```
ansible-galaxy gurnama -r talaplary.yml
```

1. Ansible oýun kitabyny işlediň:

```
ansible-playbook site_training.yml -i inwentar/ training.yml -e ansible_become_password ='XroadPKI123!' --  
limit training.ca3.pki.gov.tm
```

EJBCA we SignServer-i täzelemek

1. Çykyş belliklerini okaň!
2. <https://hub.docker.com>
3. Ikisinde-de surat wersiýasyny üýtget

topar_wars/base/app_ca.yml

topar_wars/base/app_tsa.yml

1. Ansible oýun kitabyňy işlediň

```
ansible-playbook site_training.yml -i inwentar/training.yml -e ansible_become_password='XroadPKI123!' --limit training1.ca.pki.gov.tm -t app_ca_post
```