Kā uzģenerēt Publisko atslēgu (sertifikātu), izmantojot Java keytool rīku.

Instrukcijas un sīkāks apraksts par sertifikātu ģenerēšanas procesu, izmantojot Java keytool rīku pieejama šajā adresē: http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html

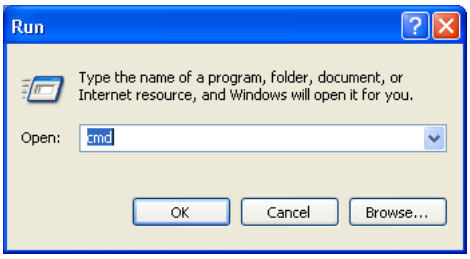
Citadele bankas prasības sertifikātam ir sekojošas:

Algoritms:	SHA256withRSA
Publiskās atslēgas kodēšanas algoritms:	RSA
Publiskās atslēgas garums:	4096
Maksimālais sertifikāta derīguma termiņš:	2 gadi

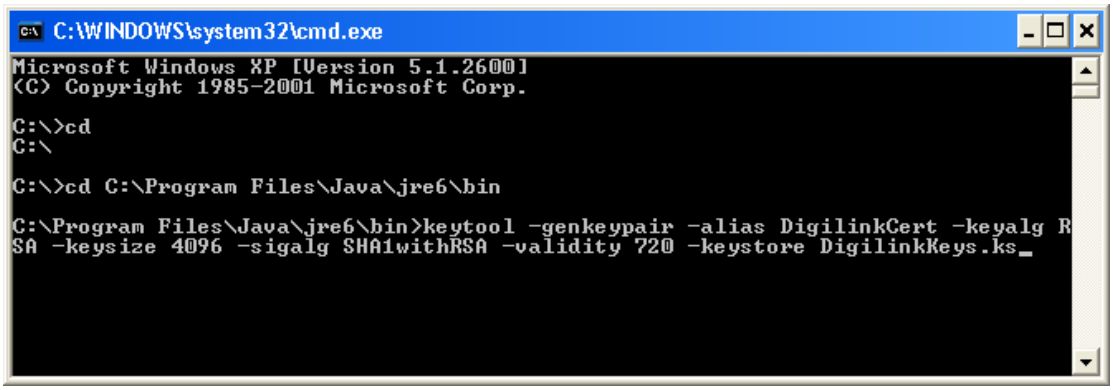
1. Pirmais solis ir uzģenerēt sertifikātu.

Izsauciet komandrindu un ierakstiet tajā sekojošu pieprasījumu:

keytool -genkeypair -alias [sertifikāta nosaukums sertifikātu glabātuvē] -keyalg RSA -keysize 4096 -sigalg SHA1withRSA -validity [sertifikāta derīguma termiņš dienās] -keystore [Sertifikātu glabātuves nosaukums.ks]



Piemērs: keytool -genkeypair -alias DigilinkCert -keyalg RSA -keysize 4096 -sigalg SHA256withRSA -validity 720 -keystore DigilinkKeys.ks



Programma liks ievadīt sertifikāta ģerēšanai nepieciešamo informāciju –

Enter keystore password: ****** Uzstādiet sertifikātu glabātuves paroli (min 6 simboli)
Re-enter new password: ****** Atkārtojiet sertifikātu glabātuves paroli
What is your first and last name? (Ievadiet vārdu, uzvārdu)
 [Unknown]: Janis Berzins
What is the name of your organizational unit? (Ievadiet struktūrvienības nosaukumu)
 [Unknown]: IT
What is the name of your organization? (Ievadiet uzņēmuma nosaukumu)
 [Unknown]: SIA ABC
What is the name of your City or Locality? (Ievadiet pilsētu)
 [Unknown]: Riga
What is the name of your State or Province? (Ievadiet valsti)
 [Unknown]: Latvia
What is the two-letter country code for this unit? (Ievadiet valsts kodu)
 [Unknown]: LV
Is CN=Janis Berzins, OU=IT, O=SIA ABC, L=Riga, ST=Latvia, C=LV correct? (apstipriniet savu izvēli)
 [no]: yes (ja viss ievadīts pareizi, apstipriniet to ar YES)

Enter key password for <DigilinkCert> ****** (uzstādiet paroli sertifikātam)
	(RETURN if same as keystore password):
Re-enter new password: ****** (atkārtojiet sertifikāta paroli)

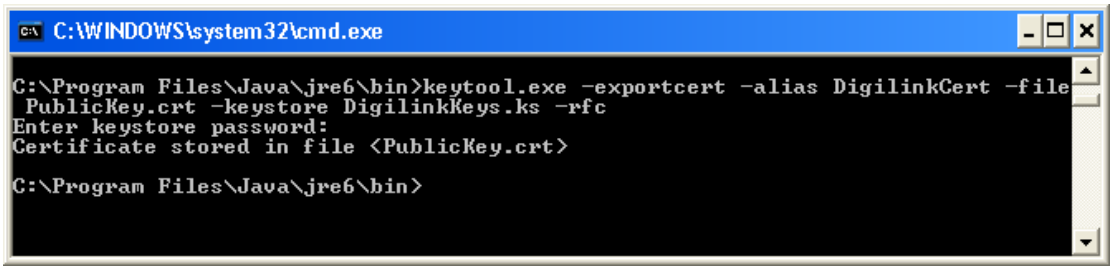
Šī piemēra rezultāta tiks izveidota sertifikātu glabātuve DigilinkKeys.ks un tajā noglabāts sertifikāts DigilinkCert.

2. Nākamais solis ir izeksportēt no sertifikāta publisko atslēgu, kas ir jāatsūta uz Banku. Publiskā atslēga Bankai nepieciešama, lai pārbaudītu no Uzņēmuma saņemto ziņojumu (maksājumu pieprasījumu) autentiskumu.

Šim nolūkam ierakstiet sekojošu komandu:

keytool.exe -exportcert -alias [iepriekš izveidotais sertifikāta nosaukums sertifikātu glabātuvē] -file [Eksportētās atslēgas faila nosaukums.crt] -keystore [iepriekš izveidotās sertifikātu glabātuves nosaukums.ks] –rfc

Piemērs:
keytool.exe -exportcert -alias DigilinkCert -file PublicKey.crt -keystore DigilinkKeys.ks -rfc



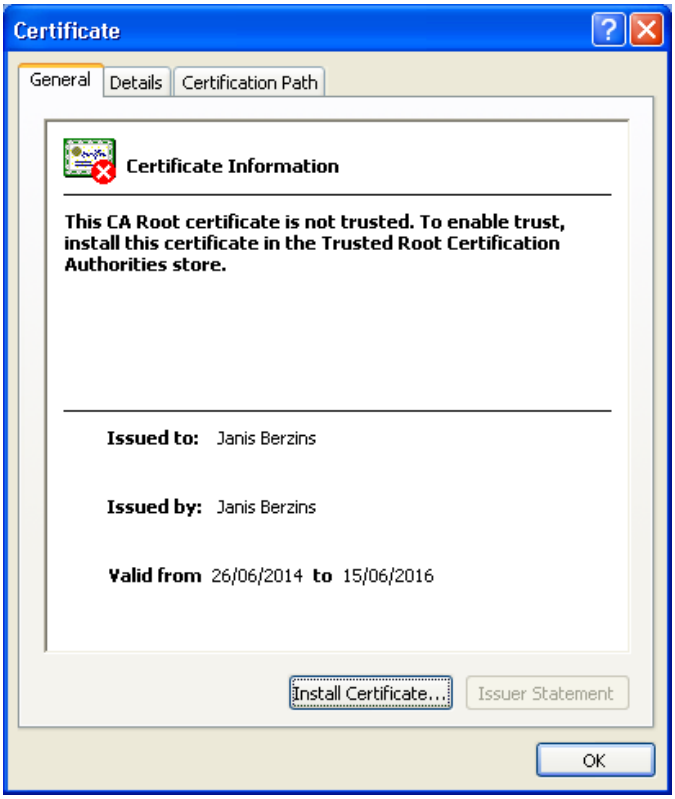
Programma lūgs jūs ievadīt sertifikāta glabātuves paroli, kuru Jūs izveidojāt 1.solī:

Enter keystore password: ******
Certificate stored in file <PublicKey.crt> - ar šo sertifikāts ir izeksportēts failā PublicKey.crt tajā direktorijā, kurā strādājat, un to ir iespējams atsūtīt uz Banku kā e-pasta pielikumu. Ja sertifikātu sistēma neļauj sūtīt, tas ir jāsaarhivē.

Fails izskatās sekojoši:


PublicKey.crt

Failu atverot, informācija izskatās sekojoši:



Fails, atvērts ar Notepad, izskatās sekojoši:

-----BEGIN CERTIFICATE-----
MIIFRDCCAyygAwIBAgIEU6wWRTANBgkqhkiG9w0BAQUFADBkMQswCQYDVQQGEwJMVjEPMA0GA1UE
CBMGTGF0dmlhMQ0wCwYDVQQHEwRSaWdhMRAwDgYDVQQKEwdTSUEgQUJDMQswCQYDVQQLEwJJVDEW
MBQGA1UEAxMNSmFuaXMgQmVyemluczAeFw0xNDA2MjYxMjQ3MDFaFw0xNjA2MTUxMjQ3MDFaMGQx
CzAJBgNVBAYTAkxWMQ8wDQYDVQQIEwZMYXR2aWExDTALBgNVBAcTBFJpZ2ExEDAOBgNVBAoTB1NJ
QSBBQkMxCzAJBgNVBAsTAklUMRYwFAYDVQQDEw1KYW5pcyBCZXJ6aW5zMIICIjANBgkqhkiG9w0B
.....
Y6z4MD8pKTJNCr/ZWT7ii/57fJ9sVh+Iht/kqX/y6klow30yPxLJ37LPL+IPe3iyf/WpVoMNOmy5
V/3x7KL/Rv1ASaBuyjdIRuSb7e3a9MPBgT01xr/sOUI4jg2+4UZtmKuPqJx0OcVaInPbWI8XnzOQ
0IkaDLQfnj/UsldRcLLadW8KyVpbw+2qAhRw+p25gBx95vvDFO6c/YkTUqUxaWmZoj44/lUe6pf6
t0QA2e4Ay5zUYZHFdL42IT01qm2HGn4/M/E8Plw8QLlgcWoVrFNvE37Xm+N6JuMw/w33NmBZ8ndM
jRM976kfCBr+wxHlSuL0z9PZCZhTZDvzxVG70N/PEdTOLz9UGRqmKl0=
-----END CERTIFICATE-----