Hoe kan trust management effectief worden geïmplementeerd voor het beveiligen van bedrijven met heterogene gesegmenteerde netwerken?

Thibo Haezaert.

Scriptie voorgedragen tot het bekomen van de graad van
Professionele bachelor in de toegepaste informatica

Promotor: Dhr. G. Blondeel
Co-promotor: Dhr. D. Mussen
Academiejaar: 2024–2025
Eerste examenperiode

Departement IT en Digitale Innovatie .

HO
GENT

Woord vooraf

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Samenvatting

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

Lijst van codefragmenten

1

Inleiding

De inleiding moet de lezer net genoeg informatie verschaffen om het onderwerp te begrijpen en in te zien waarom de onderzoeksvraag de moeite waard is om te onderzoeken. In de inleiding ga je literatuurverwijzingen beperken, zodat de tekst vlot leesbaar blijft. Je kan de inleiding verder onderverdelen in secties als dit de tekst verduidelijkt. Zaken die aan bod kunnen komen in de inleiding (**Pollefliet2011**):

- context, achtergrond
- afbakenen van het onderwerp
- verantwoording van het onderwerp, methodologie
- probleemstelling
- onderzoeksdoelstelling
- onderzoeksvraag
- ...

1.1. Probleemstelling

Uit je probleemstelling moet duidelijk zijn dat je onderzoek een meerwaarde heeft voor een concrete doelgroep. De doelgroep moet goed gedefinieerd en afgelijnd zijn. Doelgroepen als “bedrijven,” “KMO’s”, systeembeheerders, enz. zijn nog te vaag. Als je een lijstje kan maken van de personen/organisaties die een meerwaarde zullen vinden in deze bachelorproef (dit is eigenlijk je steekproefkader), dan is dat een indicatie dat de doelgroep goed gedefinieerd is. Dit kan een enkel bedrijf zijn of zelfs één persoon (je co-promotor/opdrachtgever).

1.2. Onderzoeksvraag

Wees zo concreet mogelijk bij het formuleren van je onderzoeksvraag. Een onderzoeksvraag is trouwens iets waar nog niemand op dit moment een antwoord heeft (voor zover je kan nagaan). Het opzoeken van bestaande informatie (bv. "welke tools bestaan er voor deze toepassing?") is dus geen onderzoeksvraag. Je kan de onderzoeksvraag verder specifiëren in deelvragen. Bv. als je onderzoek gaat over performantiemetingen, dan

1.3. Onderzoeksdoelstelling

Wat is het beoogde resultaat van je bachelorproef? Wat zijn de criteria voor succes? Beschrijf die zo concreet mogelijk. Gaat het bv. om een proof-of-concept, een prototype, een verslag met aanbevelingen, een vergelijkende studie, enz.

1.4. Opzet van deze bachelorproef

De rest van deze bachelorproef is als volgt opgebouwd:
In Hoofdstuk 2 wordt een overzicht gegeven van de stand van zaken binnen het onderzoeksdomein, op basis van een literatuurstudie.
In Hoofdstuk 3 wordt de methodologie toegelicht en worden de gebruikte onderzoekstechnieken besproken om een antwoord te kunnen formuleren op de onderzoeksvragen.
In Hoofdstuk 4, tenslotte, wordt de conclusie gegeven en een antwoord geformuleerd op de onderzoeksvragen. Daarbij wordt ook een aanzet gegeven voor toekomstig onderzoek binnen dit domein.

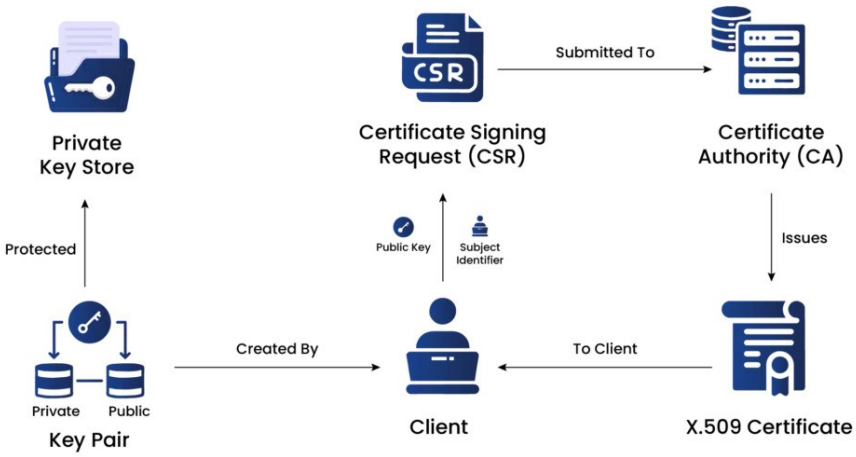
2

Stand van zaken

Om het onderzoeksonderwerp samen met de achterliggende uitdaging te begrijpen, is het belangrijk om de werking van een Public Key Infrastructure (PKI) te begrijpen. Thales (2025) definieert een PKI als een set van hardware, software, policies, processen en procedures die noodzakelijk zijn voor het maken, beheren, uitgeven, gebruiken, opslaan en intrekken van digitale certificaten en publieke keys. PKI's zijn de basis die het gebruik van technologieëen zoals digitale handtekeningen en encryptie mogelijk maakt over een grote populatie van gebruikers. Zij helpen namelijk met het vaststellen van de identiteit van personen, apparaten en diensten, wat gecontrolleerde toegang tot systemen en bronnen alsook data beveiliging en controle mogelijk maakt.

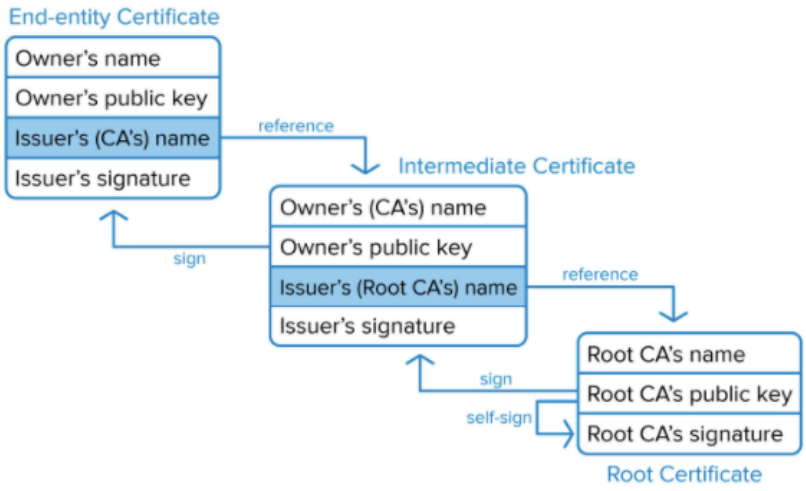
Een groot deel van PKI's zijn Digitale Certificaten en Certificate Authorities (CA's). Een certificate authority is een bedrijf of organisatie die de identiteit van entiteiten (zoals websites, e-mail adressen, bedrijven, individuen, enz.) valideert en ze vastbindt aan cryptografische sleutels door middel van het uitgeven van electronische documenten gekend als digitale certificaten. Deze certificaten brengen een aantal functionaliteiten zoals: authenticatie, Encryptie en integriteit. Authenticatie: Een certificaat doet zich voor als een getuigschrift dat de identiteit valideert van de entiteit waaraan het is uitgegeven. Encryptie: Een certificaat kan gebruikt worden voor beveiligde communicatie over onbeveiligde netwerken zoals het internet. Integriteit: Een certificaat kan via digitale handtekeningen de integriteit van documenten verzekeren zodanig ze niet gewijzigd kunnen worden door een derde partij tijdens de transmissie. Deze certificaten zorgen dus voor een beveiligde en geëncrypteerde communicatie tussen 2 partijen via public key cryptografie. (SSL.com, 2024)

Wanneer een certificaat wordt aangevraagd bij een CA, moet de aanvrager eerst een public en private key genereren. De private key moet onder de controle en



Figuur 2.1: Deze afbeelding toont de stappen en componenten in het certificaat uitgave proces.

eigendom van de aanvrager blijven. In sommige gevallen worden de private keys gegenereerd en veilig bewaart in een Hardware Security Module (HSM) die behoort tot de CA. (SSL.com, 2024) Om de registratie van certificaten te starten, maakt de aanvrager een Certificate Signing Request (CSR) aan. Deze CSR bevat de public key en andere informatie van de aanvrager die in het certificaat zal worden opgenomen, zoals de domeinnaam voor een SSL/TLS certificaat of de aanvrager's e-mail adres voor een S/MIME certificaat. Daarna wordt de CSR ingedient bij de CA. De CA zal de identiteit van de aanvrager samen met de bijkomende informatie verifiëren. De CA kan verschillende manieren gebruiken om de aanvrager zijn identiteit te verifiëren, zoals e-mail verificatie, domein validatie of manuele validatie van juridische documenten. Wanneer de CA het verificatie proces heeft voltooid en vaststelt dat de aanvrager legitiem is, zal het digitale certificaat worden uitgegeven. Het certificaat zal de aanvrager zijn public key en bijkomende informatie bevatten, alsook een geldigheidstermijn en de digitale handtekening van de CA. Het uitgegeven certificaat wordt dan terug gebracht naar de aanvrager, afhankelijk van de CA en het certificaat type zal het certificaat geleverd worden op een verschillende manier zoals via e-mail, een beveiligd portaal of een andere methode. Na het ontvangen van het certificaat is het aan de aanvrager om het certificaat te installeren op de toepasselijke server of apparaat waar het zal worden gebruikt. Als voorbeeld, een SSL/TLS certificaat wordt geïnstalleerd op een webserver voor een beveiligde connectie naar een website. Eenmaal het certificaat is geïnstalleerd, kan het gebruikt worden voor protocolen die verantwoordelijk zijn voor beveiligde communicatie. Clients, gebruikers of andere entiteiten die in contact komen met de certificaat eigenaar kunnen de authenticiteit van het certificaat verifiëren aan de hand van de CA zijn digitale handtekening, wat een beveiligde en betrouwbare connectie verzekerd. Zoals eerder vermeld hebben deze certificaten een geldigheidstermijn (meestal 1 tot



Figuur 2.2: Deze afbeelding toont de ketting van vertrouwen die de client nakijkt tijdens het verifiëren van een certificaat.

2 jaren). Voor ze vervallen, moet de aanvrager het certificaat vernieuwen via een gelijkaardig proces om het te kunnen blijven gebruiken zonder onderbrekingen. (EncryptionConsulting, 2025)

Het verifiëren van een certificaat om de bepalen of het vertrouwd kan worden is belangrijk voor de veiligheid van de communicatie. Okta (2023) zegt dat tijdens een SSL/TLS handshake, de client het certificaat van de server ontvangt. De client controleert of het certificaat nog niet vervallen is en dat de domeinnaam en IP adres op het certificaat gelijkaardig zijn aan dat van de server. Daarna zal de client kijken of het certificaat correct is ondertekend door een vertrouwde CA. In de meeste gevallen zal de server certificate niet ondertekend zijn door de root CA die door de client wordt vertrouwd. In plaats van de root CA zal de client 1 of meerdere intermediate CA's vertrouwen zolang als hun ketting van vertrouwen terug leidt naar een root CA die de client vertrouwd.
Voor elke intermediate CA certificate doet de client hetzelfde verificatie proces waarbij de uitgever (issuer) zijn naam overeenkomt met de certificate eigenaar zijn naam van de volgende certificate in de ketting. Ook wordt de digitale signatuur en public key van het certificaat bekeken om te kijken of deze correct is ondertekend. Dit proces herhaald zichzelf tot de client komt bij een self-signed root CA certificate die de client vertrouwd. Op dit moment heeft de client dan een cryptografische ketting van vertrouwen gemaakt tot de server en kan de SSL/TLS handshake verder gaan.

Bij dit verificatie proces eindigt de client steeds bij een root CA certificaat die door de client moet worden vertrouwd. Om te bepalen welke root CA's door de client worden vertrouwd bestaan er trust stores. Een trust store is een collectie van root

certificaten die standaard worden vertrouwd door een client en worden beheerd door bedrijven die de client zijn operating system of browser ontwikkelen, zoals Microsoft, Mozilla en Google. Elke vendor heeft zijn eigen standaarden voor root certificaten maar ze vereisen allemaal dat een uitgevende CA een of meerdere controles ondergaan om hun vertrouwbaarheid, validiteit en conformiteit vast te stellen via de CA/B Forum Baseline Requirements vooraleer ze worden opgenomen in hun trust store. (Arampatzis, 2020) Over al de trust stores van deze vendors zijn er heel wat certificaten die niet noodzakelijk zijn. Een studie van Perl e.a. (2014) toont dat alleen maar 66% van de certificaten in de trust store van Windows, Linux, MacOS, Firefox, iOS and Android noodzakelijk zijn voor het vertrouwen van websites. Dit zorgt ervoor dat de overige derde van de root certificaten in de trust stores een potentieel veiligheidsrisico vormen voor de client.

Als oplossing hierop kunnen bedrijven het overwegen om deze standaard trust stores af te wijzen. In de plaats daarvan kunnen ze best hun eigen aangepaste, corporate-level trust store maken en gebruik maken van certificate white-listing om te bepalen welke root certificates hierin kunnen opgenomen worden. Dit helpt bedrijven met het aanvals oppervlak te verkleinen door het limiteren van de hoeveelheid vertrouwde CA's en het markeren van niet-vertrouwde SSL/TLS sessies. Organisaties kunnen dan deze certificate whitelist en blacklist updaten op een regelmatige basis afhankelijk van benoodigdheden van hun evoluerende business requirements en groeiend CA landschap. (Arampatzis, 2020)
Het beheren van deze trust stores kan een uitdaging zijn voor bedrijven, zeker bedrijven met heterogene netwerken (netwerken die clients hebben met verschillende operating systemen en browsers). Reddy en Wallace (2010) weerlegt dit door te zeggen dat deze trust anchors (Root CA certificaten) vaak bewaart worden in applicatie-specifieke of OS-specifieke trust stores. Vaak heeft dan 1 machine een verschillend aantal trust stores die niet gesynchroniseerd zijn met elkaar.

De uitdagingen hier zijn dus het vermijden van overbodige vertrouwde root certificaten binnen een netwerk en zijn segmenten afhankelijk van de business requirements en het beheren van deze trust stores over verschillende machines en applicaties.
Voor het implementeren van een oplossing voor deze uitdagingen is het van belang om te weten hoe de truststores van de verschillende operating systemen en browsers werken en hoe deze kunnen worden beheerd.

Windows heeft een truststore die de Trusted Root Certification Authorities store heet. In de officiële documentatie van Microsoft vermeld Microsoft (2024) dat de Trusted Root Certificate Authorities store op een Windows computer via de Microsoft Management Console (MMC) kan worden beheerd door de Certificate Manager

snap-in te gebruiken. De Microsoft Management Console kan worden geopend door het commando `mmc.exe` uit te voeren in deen Run dialog. In het MCC venster kan men via file -> Add/Remove Snap-in de ”Certificates” snap-in toevoegen. Hierna kan men dan in het MCC venster onder ”Certificates (local computer)” -> ”Trusted Root Certification Authorities” de lijst van vertrouwde root certificaten bekijken en beheren. Microsoft (2024) vermeld ook dat standaard de Trusted Root Certificate Authorities store geconfigureerd is met een aantal publieke CA’s die de vereisten van de Microsoft Root Certificate Program hebben voltooid.

Naast de GUI manier van beheren van de truststore, biedt Microsoft ook een manier om het te beheren via de command line aan de hand van het certutil commando. Certutil.exe is een command-line programma geinstalleerd als onderdeel van de Certitifate Services. Certutil.exe kan gebruikt worden voor het tonen van certificate authority (CA) configuratie informatie, het configureren van Certificate Services en CA componenten te back-uppen en te herstellen. Dit programma kan ook certificaten, key pairs en certificate chains verifiëren. (Microsoft, 2025) Om een certificate store te tonen aan de hand van certutil kan het volgende commando worden gebruikt:

```
certutil [options] -store [CertificateStoreName [CertId
↪ [OutputFile]]]
```

Waar CertificateStoreName de naam is van de certificate store, CertId de match token is van het certificaat en OutputFile de naam is van het bestand waarin de overeenkomende certificaten worden opgeslagen. (Microsoft, 2025)
Om een certificaat toe te voegen aan een certificate store kan het volgende commando worden gebruikt:

```
certutil [options] -addstore CertificateStoreName InFile
```

Waar CertificateStoreName de naam is van de certificate store en InFile de certificate file is die moet worden toegevoegd. (Microsoft, 2025)
Linux heeft niet zoals Windows één centrale trust store. In plaats daarvan heeft Linux verschillende trust stores die afhankelijk zijn van de applicatie of het OS.
Binnen Ubuntu Server moet een certificaat in PEM formaat staan vooraleer het kan worden toegevoegd aan de trust store. Om een PEM-geformatteerd root CA certificaat met als naam ”local-ca.crt” te installeren in de trust store van Ubuntu Server kan het volgende commando worden gebruikt:

```
sudo apt-get install -y ca-certificates
sudo cp local-ca.crt /usr/local/share/ca-certificates
```

```
3 sudo update-ca-certificates
```

Het is hierbij belangrijk dat het certificaat bestand de extensie .crt heeft anders zal het niet worden verwerkt.
De CA trust store (die gegenereerd wordt door update-ca-certificates) is te vinden op de volgende locaties:

- Als een file (PEM bundel) in /etc/ssl/certs/ca-certificates.crt
- Als een OpenSSL-compatibele certificaat directory in /etc/ssl/certs/ca-certificates.pem

(Canonical, 2025)

Red Hat Enterprise Linux (RHEL) heeft een andere manier van het beheren van de trust store. RHEL biedt de Shared System Certificates aan. De Shared System Certificates opslag laat NSS, GnuTLS, OpenSSL en Java toe om een standaard bron te delen voor het ophalen van systeem certificate anchors en black list informatie. Standaard bevat de truststore de Mozilla CA list, die positieve en negatieve vertrouwen informatie bevat. Het systeem laat toe om de Mozilla CA lijst aan te passen of om een andere CA lijst te gebruiken. (Red Hat, 2024)

In Red Hat Enterprise Linux 7 is de systeem-brede truststore te vinden in de directories /etc/pki/ca-trust/ en /usr/share/pki/ca-trust-source/ . De trust settings in /usr/share/pki/ca-trust-source/ worden behandeld met een lagere prioriteit dan de settings in /etc/pki/ca-trust/ . Certificaat bestanden worden anders behandeld afhankelijk van de subdirectory waarin ze worden geplaatst:

- /usr/share/pki/ca-trust-source/anchors/ of /etc/pki/ca-trust/source/anchors/ : voor trust anchors.
- /usr/share/pki/ca-trust-source/blacklist/ of /etc/pki/ca-trust/source/blacklist/ : voor niet vertrouwde certificaten.
- /usr/share/pki/ca-trust-source/ of /etc/pki/ca-trust/source/ : voor certificaten in de extended BEGIN TRUSTED bestandsformaat.

(Red Hat, 2024)
Om een certificaat in de simpele PEM of DER bestandsformaten aan de lijst van vertrouwde CA's op het systeem toe te voegen, kan je simpelweg het certificaat bestand kopiëren naar de /usr/share/pki/ca-trust-source/anchors/ of /etc/pki/ca-trust/source/anchors/ directory. Om de systeem-brede truststore te updaten ka je het update-ca-trust commando gebruiken zoals volgt:

```
1 cp ~/certificate-trust-examples/Cert-trust-test-ca.pem
  ↪ /usr/share/pki/ca-trust-source/anchors/
```

```
update-ca-trust
```

Om de trust anchors op te lijsten, toe te voegen, veranderen of verwijderen kan het 'trust' commando gebruikt worden. Voor het oplijsten van de trust anchors wordt 'trust list' gebruikt. Een trust anchor opslaan in de trust store kan met het 'trust anchor' sub-commando en het specifiëren van het pad (vb.: path.to) naar het certificaat bestand, zoals volgt:

```
trust anchor path.to/certificate.crt
```

Om een trust anchor te verwijderen kan een pad naar het certificaat of ID van het certificaat gebruikt worden:

```
trust anchor --remove path.to/certificate.crt
trust anchor --remove "pkcs11:id=%AA%BB%CC%DD%EE;type=cert"
```

(Red Hat, 2024)

Applicaties kunnen ook hun eigen trust store hebben. Een voorbeeld hiervan is Mozilla Firefox. Firefox maakt gebruik van de NSS (Network Security Services) library voor het beheren van de trust store. De Network Security Services (NSS) library is een set van libraries ontwikkeld om cross-platform ontwikkeling van veilige client en server applicaties te ondersteunen. De libraries ondersteunen SSL v3, TLS, PKCS 5, PKCS 7, PKCS 11, PKCS 12, S/MIME, X.509 v3 certificaten en andere security standaarden. /autociteNSS Firefox geeft bij initiatie een string met pad naar de directory waar NSS de security en configuratie data mag opslaan. NSS slaat 3 bestanden op in die directory:

- cert8.db: slaat publiek toegankelijke objecten op (Certificaten, CRL's, S/MIME records).
- key3.db: slaat private keys op.
- secmod.db: slaat de PKCS11 module configuratie op.

Als in deze directory grote security objecten zitten (zoals grote CRL's), zal NSS deze opslaan in bestanden in subdirectories genaamd 'cert8.dir'. In het geval dat cert8.db en/of key3.db niet bestaan, zal NSS de data lezen van oudere versies vand eze databases (bv.: cert7.db, cert6.db,...) en zal deze data gebruiken om een nieuwe cert8.db en key3.db te maken. (Mozilla, 2018)
Ook beweert Mozilla (2024) dat standaard Firefox op Windows, MacOS en Android zal zoeken en gebruik maken van de third-party CA's die zijn opgenomen in de operating system zijn trust store. Firefox kan geconfigureerd worden om automatisch

te zoeken naar CA's die in de Windows certificate store zijn toegevoegd door een gebruiker of administrator. Dit kan gedaan worden door de security.enterprise_roots.enabledoptieinteste

HKLM/SOFTWARE/Policies/Microsoft/SystemCertificates/Root/Certificates (pad in API flag CERT_SYSTEM_STORE_LOCAL_MACHINE_GROUP_POLICY)
HKLM/SOFTWARE/Microsoft/EnterpriseCertificates/Root/Certificates (pad in API flag CERT_SYSTEM_STORE_LOCAL_MACHINE_ENTERPRISE)
(Mozilla, 2024)

TextciteMozillaCA voorziet ook dat enterprise policies kunnen gebruikt worden voor het toevoegen van CA certificaten in Firefox. De 'ImportEnterpriseRoots' key op 'true' zetten, zorgt ervoor dat Firefox root certificaten zal vertrouwen. De 'Install' key zoekt standaard naar certificaten in de onderstaande locaties. Er kan ook een specifiek pad worden opgegeven. Als Firefox daar geen certificaten vindt zal het de standaard directories bekijken:

- Windows
  - %USERPROFILE%
    AppData
    Local
    Mozilla
    Certificates
  - %USERPROFILE%
    AppData
    Roaming
    Mozilla
    Certificates
- macOS
  - /Library/Application Support/Mozilla/Certificates
  - /Library/Application Support/Mozilla/Certificates
- Linux
  - /usr/lib/mozilla/certificates
  - /usr/lib64/mozilla/certificates

(Mozilla, 2024)

Java heeft ook zijn eigen trust store.

3

Methodologie

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

Maecenas non massa. Vestibulum pharetra nulla at lorem. Duis quis quam id lacus dapibus interdum. Nulla lorem. Donec ut ante quis dolor bibendum

condimentum. Etiam egestas tortor vitae lacus. Praesent cursus. Mauris bibendum pede at elit. Morbi et felis a lectus interdum facilisis. Sed suscipit gravida turpis. Nulla at lectus. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Praesent nonummy luctus nibh. Proin turpis nunc, congue eu, egestas ut, fringilla at, tellus. In hac habitasse platea dictumst.

Vivamus eu tellus sed tellus consequat suscipit. Nam orci orci, malesuada id, gravida nec, ultricies vitae, erat. Donec risus turpis, luctus sit amet, interdum quis, porta sed, ipsum. Suspendisse condimentum, tortor at egestas posuere, neque metus tempor orci, et tincidunt urna nunc a purus. Sed facilisis blandit tellus. Nunc risus sem, suscipit nec, eleifend quis, cursus quis, libero. Curabitur et dolor. Sed vitae sem. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Maecenas ante. Duis ullamcorper enim. Donec tristique enim eu leo. Nullam molestie elit eu dolor. Nullam bibendum, turpis vitae tristique gravida, quam sapien tempor lectus, quis pretium tellus purus ac quam. Nulla facilisi.

4

Conclusie

Curabitur nunc magna, posuere eget, venenatis eu, vehicula ac, velit. Aenean ornare, massa a accumsan pulvinar, quam lorem laoreet purus, eu sodales magna risus molestie lorem. Nunc erat velit, hendrerit quis, malesuada ut, aliquam vitae, wisi. Sed posuere. Suspendisse ipsum arcu, scelerisque nec, aliquam eu, molestie tincidunt, justo. Phasellus iaculis. Sed posuere lorem non ipsum. Pellentesque dapibus. Suspendisse quam libero, laoreet a, tincidunt eget, consequat at, est. Nullam ut lectus non enim consequat facilisis. Mauris leo. Quisque pede ligula, auctor vel, pellentesque vel, posuere id, turpis. Cras ipsum sem, cursus et, facilisis ut, tempus euismod, quam. Suspendisse tristique dolor eu orci. Mauris mattis. Aenean semper. Vivamus tortor magna, facilisis id, varius mattis, hendrerit in, justo. Integer purus.

Vivamus adipiscing. Curabitur imperdiet tempus turpis. Vivamus sapien dolor, congue venenatis, euismod eget, porta rhoncus, magna. Proin condimentum pretium enim. Fusce fringilla, libero et venenatis facilisis, eros enim cursus arcu, vitae facilisis odio augue vitae orci. Aliquam varius nibh ut odio. Sed condimentum condimentum nunc. Pellentesque eget massa. Pellentesque quis mauris. Donec ut ligula ac pede pulvinar lobortis. Pellentesque euismod. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent elit. Ut laoreet ornare est. Phasellus gravida vulputate nulla. Donec sit amet arcu ut sem tempor malesuada. Praesent hendrerit augue in urna. Proin enim ante, ornare vel, consequat ut, blandit in, justo. Donec felis elit, dignissim sed, sagittis ut, ullamcorper a, nulla. Aenean pharetra vulputate odio.

Quisque enim. Proin velit neque, tristique eu, eleifend eget, vestibulum nec, lacus. Vivamus odio. Duis odio urna, vehicula in, elementum aliquam, aliquet laoreet, tellus. Sed velit. Sed vel mi ac elit aliquet interdum. Etiam sapien

neque, convallis et, aliquet vel, auctor non, arcu. Aliquam suscipit aliquam lectus. Proin tincidunt magna sed wisi. Integer blandit lacus ut lorem. Sed luctus justo sed enim.

Morbi malesuada hendrerit dui. Nunc mauris leo, dapibus sit amet, vestibulum et, commodo id, est. Pellentesque purus. Pellentesque tristique, nunc ac pulvinar adipiscing, justo eros consequat lectus, sit amet posuere lectus neque vel augue. Cras consectetuer libero ac eros. Ut eget massa. Fusce sit amet enim eleifend sem dictum auctor. In eget risus luctus wisi convallis pulvinar. Vivamus sapien risus, tempor in, viverra in, aliquet pellentesque, eros. Aliquam euismod libero a sem.

Nunc velit augue, scelerisque dignissim, lobortis et, aliquam in, risus. In eu eros. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Curabitur vulputate elit viverra augue. Mauris fringilla, tortor sit amet malesuada mollis, sapien mi dapibus odio, ac imperdiet ligula enim eget nisl. Quisque vitae pede a pede aliquet suscipit. Phasellus tellus pede, viverra vestibulum, gravida id, laoreet in, justo. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Integer commodo luctus lectus. Mauris justo. Duis varius eros. Sed quam. Cras lacus eros, rutrum eget, varius quis, convallis iaculis, velit. Mauris imperdiet, metus at tristique venenatis, purus neque pellentesque mauris, a ultrices elit lacus nec tortor. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent malesuada. Nam lacus lectus, auctor sit amet, malesuada vel, elementum eget, metus. Duis neque pede, facilisis eget, egestas elementum, nonummy id, neque.

A

Onderzoeksvoorstel

Het onderwerp van deze bachelorproef is gebaseerd op een onderzoeksvoorstel dat vooraf werd beoordeeld door de promotor. Dat voorstel is opgenomen in deze bijlage.

A.1. Inleiding

Waarover zal je bachelorproef gaan? Introduceer het thema en zorg dat volgende zaken zeker duidelijk aanwezig zijn:

- kaderen thema
- de doelgroep
- de probleemstelling en (centrale) onderzoeksvraag
- de onderzoeksdoelstelling

Denk er aan: een typische bachelorproef is *toegepast onderzoek*, wat betekent dat je start vanuit een concrete probleemsituatie in bedrijfscontext, een **casus**. Het is belangrijk om je onderwerp goed af te bakenen: je gaat voor die *ene specifieke probleemsituatie* op zoek naar een goede oplossing, op basis van de huidige kennis in het vakgebied.

De doelgroep moet ook concreet en duidelijk zijn, dus geen algemene of vaag gedefinieerde groepen zoals *bedrijven*, *developers*, *Vlamingen*, enz. Je richt je in elk geval op it-professionals, een bachelorproef is geen populariserende tekst. Eén specifiek bedrijf (die te maken hebben met een concrete probleemsituatie) is dus beter dan *bedrijven* in het algemeen.

Formuleer duidelijk de onderzoeksvraag! De begeleiders lezen nog steeds te veel voorstellen waarin we geen onderzoeksvraag terugvinden.

Schrijf ook iets over de doelstelling. Wat zie je als het concrete eindresultaat van je onderzoek, naast de uitgeschreven scriptie? Is het een proof-of-concept, een rapport met aanbevelingen, ...Met welk eindresultaat kan je je bachelorproef als een succes beschouwen?

A.2. Literatuurstudie

Hier beschrijf je de *state-of-the-art* rondom je gekozen onderzoeksdomein, d.w.z. een inleidende, doorlopende tekst over het onderzoeksdomein van je bachelorproef. Je steunt daarbij heel sterk op de professionele *vakliteratuur*, en niet zozeer op populariserende teksten voor een breed publiek. Wat is de huidige stand van zaken in dit domein, en wat zijn nog eventuele open vragen (die misschien de aanleiding waren tot je onderzoeksvraag!)?

Je mag de titel van deze sectie ook aanpassen (literatuurstudie, stand van zaken, enz.). Zijn er al gelijkaardige onderzoeken gevoerd? Wat concluderen ze? Wat is het verschil met jouw onderzoek?

Verwijs bij elke introductie van een term of bewering over het domein naar de vakliteratuur, bijvoorbeeld (Hykes, 2013)! Denk zeker goed na welke werken je refereert en waarom.

Draag zorg voor correcte literatuurverwijzingen! Een bronvermelding hoort thuis *binnen* de zin waar je je op die bron baseert, dus niet er buiten! Maak meteen een verwijzing als je gebruik maakt van een bron. Doe dit dus *niet* aan het einde van een lange paragraaf. Baseer nooit teveel aansluitende tekst op eenzelfde bron.

Als je informatie over bronnen verzamelt in JabRef, zorg er dan voor dat alle nodige info aanwezig is om de bron terug te vinden (zoals uitvoerig besproken in de lessen Research Methods).

Je mag deze sectie nog verder onderverdelen in subsecties als dit de structuur van de tekst kan verduidelijken.

A.3. Methodologie

Hier beschrijf je hoe je van plan bent het onderzoek te voeren. Welke onderzoekstechniek ga je toepassen om elk van je onderzoeksvragen te beantwoorden? Gebruik je hiervoor literatuurstudie, interviews met belanghebbenden (bv. voor requirements-analyse), experimenten, simulaties, vergelijkende studie, risico-analyse, PoC, ...?

Valt je onderwerp onder één van de typische soorten bachelorproeven die besproken zijn in de lessen Research Methods (bv. vergelijkende studie of risicoanalyse)? Zorg er dan ook voor dat we duidelijk de verschillende stappen terug vinden die we verwachten in dit soort onderzoek!

Vermijd onderzoekstechnieken die geen objectieve, meetbare resultaten kunnen opleveren. Enquêtes, bijvoorbeeld, zijn voor een bachelorproef informatica meestal **niet geschikt**. De antwoorden zijn eerder meningen dan feiten en in de praktijk blijkt het ook bijzonder moeilijk om voldoende respondenten te vinden. Studenten die een enquête willen voeren, hebben meestal ook geen goede definitie van de populatie, waardoor ook niet kan aangetoond worden dat eventuele resultaten representatief zijn.

Uit dit onderdeel moet duidelijk naar voor komen dat je bachelorproef ook technisch voldoende diepgang zal bevatten. Het zou niet kloppen als een bachelorproef informatica ook door bv. een student marketing zou kunnen uitgevoerd worden.

Je beschrijft ook al welke tools (hardware, software, diensten, ...) je denkt hiervoor te gebruiken of te ontwikkelen.

Probeer ook een tijdschatting te maken. Hoe lang zal je met elke fase van je onderzoek bezig zijn en wat zijn de concrete *deliverables* in elke fase?

A.4. Verwacht resultaat, conclusie

Hier beschrijf je welke resultaten je verwacht. Als je metingen en simulaties uitvoert, kan je hier al mock-ups maken van de grafieken samen met de verwachte conclusies. Benoem zeker al je assen en de onderdelen van de grafiek die je gaat gebruiken. Dit zorgt ervoor dat je concreet weet welk soort data je moet verzamelen en hoe je die moet meten.

Wat heeft de doelgroep van je onderzoek aan het resultaat? Op welke manier zorgt jouw bachelorproef voor een meerwaarde?

Hier beschrijf je wat je verwacht uit je onderzoek, met de motivatie waarom. Het is **niet** erg indien uit je onderzoek andere resultaten en conclusies vloeien dan dat je hier beschrijft: het is dan juist interessant om te onderzoeken waarom jouw hypothesen niet overeenkomen met de resultaten.

Bibliografie

Arampatzis, A. (2020). What Is a Trust Store and How Hard Is It to Manage? *TLS certificates*. https://venafi.com/blog/what-trust-store-and-how-hard-it-manage/

Canonical. (2025). Install a root CA certificate in the trust store. *Ubuntu Server documentation*. Verkregen maart 6, 2025, van https://documentation.ubuntu.com/server/how-to/security/install-a-root-ca-certificate-in-the-trust-store/index.html

EncryptionConsulting. (2025). What is Certificate Enrollment and how is it used? Verkregen februari 26, 2025, van https://www.encryptionconsulting.com/education-center/what-is-certificate-enrollment-and-how-is-it-used/

Hykes, S. (2013, maart 21). *The future of Linux Containers (PyCon 2013)*. Verkregen september 1, 2016, van https://www.youtube.com/watch?v=wW9CAH9nSLs

Microsoft. (2024). Trusted Root Certification Authorities Certificate Store. *Microsoft Learn*. Verkregen maart 6, 2025, van https://learn.microsoft.com/en-us/windows-hardware/drivers/install/trusted-root-certification-authorities-certificate-store

Microsoft. (2025). certutil. *Microsoft Learn*. Verkregen maart 6, 2025, van https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil

Mozilla. (2018). NSS Shared DB. *Mozilla wiki*. Verkregen maart 6, 2025, van https://wiki.mozilla.org/NSS_Shared_DB

Mozilla. (2024). Set up Certificate Authorities (CAs) in Firefox. *Support Mozilla*. Verkregen maart 6, 2025, van https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox

Okta. (2023). What Is Certificate Verification for Root CA, Intermediate CA, and End-Entity CA. *Knowledge base*. Verkregen februari 26, 2025, van https://support.okta.com/help/s/article/How-can-we-do-Certificate-Verification-Need-more-explanation-for-Root-CA-Intermediate-CA-End-entity-CA?language=en_US

Perl, H., Fahl, S., & Smith, M. (2014). You Won't Be Needing These Any More: On Removing Unused Certificates from Trust Stores (N. Christin & R. Safavi-

Naini, Red.). *Financial Cryptography and Data Security*, 307–315. https://doi.org/https://doi.org/10.1007/978-3-662-45472-5_20

Red Hat. (2024). 4.14. Using Shared System Certificates. *Red Hat Documentation*. Verkregen maart 6, 2025, van https://www.redhat.com/en/blog/configure-ca-trust-list

Reddy, R., & Wallace, C. (2010, oktober 1). Trust Anchor Management Requirements. https://doi.org/10.17487/RFC6024

SSL.com. (2024). What is the Role of a Certificate Authority? *What is a Certificate Authority (CA)?* Verkregen februari 25, 2025, van https://www.ssl.com/article/what-is-a-certificate-authority-ca/

Thales. (2025). What is PKI? *What is PKI and What is it used for?* Verkregen februari 26, 2025, van https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki