ONDERZOEKSVOORSTEL

Hoe kan trust management effectief worden geïmplementeerd voor het beveiligen van het netwerk van een bank?

Bachelorproef, 2024-2025

Thibo Haezaert

E-mail: thibo.haezaert@student.hogent.be
Co-promotor: D. Mussen (KBC, dirk.mussen@kbc.be)

Samenvatting

In dit onderzoek wordt een centrale aanpak voor truststorebeheer in bankennetwerken onderzocht. Truststores, die vertrouwde root certificaten bevatten, spelen een cruciale rol in het waarborgen van veilige communicatie binnen banken. Momenteel worden truststores vaak verspreid beheerd, afhankelijk van applicaties en besturingssystemen. Deze gefragmenteerde aanpak leidt tot inefficiëntie, zoals het dupliceren van beheerprocessen waarbij beheerders handmatig wijzigingen in meerdere truststores moeten doorvoeren. Dit verhoogt de kans op fouten en leidt tot meer tijds- en middelenverlies. Het zorgt ook voor verhoogde risico's op verouderde certificaten en mogelijke beveiligingsproblemen zoals man-in-the-middle aanvallen.
Het doel van dit onderzoek is het ontwikkelen van een gecentraliseerde oplossing voor truststorebeheer, specifiek gericht op de behoeften van de financiële sector. Het onderzoek begint met een literatuurstudie naar de belangrijkste concepten van PKI, de verschillen tussen gedistribueerd en gecentraliseerd beheer, en beschikbare tools en technieken. Vervolgens wordt een virtuele bankomgeving ontworpen waarin de oplossing wordt geïmplementeerd en getest. De centrale truststorebeheeroplossing wordt geëvalueerd op veiligheid, efficiëntie en schaalbaarheid, en vergeleken met de huidige gedistribueerde aanpak.
Het onderzoek levert praktische richtlijnen en aanbevelingen op voor banken die hun truststorebeheer willen optimaliseren, met als doel een robuustere en beter beheersbare infrastructuur.

Keuzerichting: System & Network Administrator
Sleutelwoorden: Trust management, Truststore, Digital Certificates, Certificate autority

Inhoudsopgave

1. Introductie

In de digitale wereld is vertrouwen in beveiligingssystemen cruciaal, vooral binnen de financiële sector. Banken hebben complexe netwerken die moeten worden beschermd tegen cyberbedreigingen. Trust management, het beheren van vertrouwde relaties aan de hand van digitale certificaten en public key infrastructures (PKI's) speelt hierin een belangrijke rol.

Daarbij is het effectief beheren van truststores, de verzameling van vertrouwde certificaten, essentieel om veilige gegevensuitwisseling en transacties te garanderen.

In vele netwerken worden truststores verspreid beheerd, hun locatie is afhankelijk van de gebruikte applicatie of besturingssystemen. Dit leidt tot een gefragmenteerde aanpak, wat niet alleen inefficiënt is, maar ook de kans vergroot op verouderde certificaten en beveiligszwaktes.

Door een centrale aanpak te ontwikkelen voor truststorebeheer wordt er gestreefd naar meer consistentie, eenvoud en veiligheid in het beheer van certificaten. Dit onderzoek richt zich op het formuleren van richtlijnen en oplossingen die specifiek van toepassing op de behoeftes van de financiële sector.

Om dit doel te bereiken, beantwoordt dit onderzoek de volgende deelvragen:

1. Wat zijn de belangrijkste concepten en technologieën achter PKI en truststorebeheer?
2. Wat zijn de verschillen tussen gedistribueerd en gecentraliseerd truststorebeheer, en welke voordelen biedt een gecentraliseerde aanpak?
3. Welke tools en technieken worden momenteel gebruikt voor truststorebeheer, en wat zijn hun beperkingen?
4. Welke specifieke uitdagingen en eisen gelden voor truststorebeheer in bankomgevingen?
5. Welke componenten moeten worden opgenomen in een virtueel bankennetwerk om een realistisch beeld te creëren?
6. Hoe kan een gecentraliseerde oplossing voor truststorebeheer worden ontworpen en geïmplementeerd in een bankennetwerk?

7. Hoe kan de veiligheid, efficiëntie en schaalbaarheid van de gecentraliseerde oplossing worden getest en geëvalueerd?
8. In hoeverre voldoet de gecentraliseerde oplossing aan de beveiligings- en compliance-eisen van een bankomgeving?
9. Wat zijn de praktische voordelen en beperkingen van een gecentraliseerde truststorebeheeroplossing in vergelijking met een gedistribueerde aanpak?
10. Welke aanbevelingen kunnen worden gedaan voor banken die een centrale truststorebeheerstrategie willen implementeren?

Door deze vragen te beantwoorden, streeft het onderzoek ernaar richtlijnen en oplossingen te formuleren die aansluiten bij de specifieke behoeften van de financiële sector.

2. State-of-the-art

Bij het begrijpen van trust management is het belangrijk om te weten wat een public key infrastructure (PKI) en digitale certificaten zijn.

Een digitaal certificaat is een file die verbonden is met een cryptografische key pair en het authenticeert de identiteit van een website, individu, organisatie, gebruiker of apparaat. Zulke certificaten worden soms ook public key certificates of identity certificates genoemd

Een certificaat bevat het onderwerp, wat dient als de identiteit samen met een digitale signatuur. Het doel van digitale certificaten is om de identiteit en encryptie te verzekeren van een website, individu, organisatie, apparaat, gebruiker of server. (Digicert, 2025)

Een PKI beveiligd data en bouwt vertrouwen via deze digitale certificaten, die uitgegeven worden door certificate autorities (CA's) aan bedrijven nadat zij een certificate signing request (CSR) hebben gemaakt. Eens een CSR is goedgekeurd en een certificaat is uitgegeven kan een bedrijf of individu zijn communicatie, web domeinen en/of documenten authenticeren en beveiligen zolang het certificaat is gemaakt voor dit doeleinde en geldig is. (Topping, 2023)

Naast PKI en digitale certificaten zijn truststores en keystores ook van belang bij trust management.

IBM (2023) definieert dat Trust stores en keystores cryptografische artefacten bevatten, met andere woorden certificaten en private keys. Deze artefacten worden dan gebruikt door protocollen zoals TLS. Een keystore bevat persoonlijke certificaten samen met de overeenkomstige private keys die gebruikt worden om de eigenaar van het certificaat te identificeren.

Voor een TLS verbinding stelt een persoonlijk certificaat de identiteit van een endpoint voor, beide de client en de server hebben dit certificaat om elkaar te identificeren.

Een truststore bevat dan weer signer certificates die door de andere endpoints vertrouwd worden, deze certificates zijn ook gekend als "certificate autority certificates".

Deze signer certificate bevatten een public key die gebruikt wordt om een persoonlijk certificaat te valideren. Door het toevoegen van de signer certificate in de client zijn truststore, kan de client de server vertrouwen om een TLS verbinding te maken.

Vele software en besturingssystemen komen dan ook vooraf geïnstalleerd met hun eigen trust stores.

"Er zijn 4 grote organisaties die zulke trust stores beheren: 1. Microsoft root certificate program die gebruikt wordt voor Windows. 2. Apple root certificate program is gebruikt voor alle Mac apparaten. 3. De Mozilla root certificates program wordt gebruikt door Mozilla zelf en meeste Linux distributies. 4. Google root certificate program wordt gebruikt door Google chrome en andere Google applicaties."(Dwivedi, 2024)

Volgens Mervana (2024) is een van de uitdagingen voor het beheren van trust stores, dat in grote organisaties met heterogene netwerken vele trust stores gedecentraliseerd liggen waarbij er een nood is aan gecoördineerd management.

Dit kan opgelost worden door een gecentraliseerd management systeem, dit maakt het makkelijker om veranderingen te coördineren.

Andere bronnen raden zulke gecentraliseerde systemen sterk aan.

"Organisaties moeten overwegen de default trust stores af te wijzen. Ze zouden een eigen corporate-level trust store moeten maken aan de hand van certificate white-listing om te bepalen welke certificaten hierin worden opgenomen."(Arampatzis, 2020)

Bij het opstellen van deze centrale truststore binnen de financiële sector brengt dit ook enkele uitdagingen met zich mee. Er zijn namelijk beveiligingseisen voor de infrastructuur van banken waaraan moet worden voldaan.

Daarbij blijkt dat tegen het einde van 2024 de cyber security binnen europese banken moeten voldoen aan de "Digital Operational Resilience Requirements"(DORA). (Gorobeț, 2024)

Naast de DORA eisen zijn er ook nog andere eisen die van toepassing zijn op de financiële sector zoals de "Payment Services Directive 2"(PSD2).

In het onderzoek van Gounari e.a. (2024) blijkt dat PSD2 de nieuwe vereisten binnen communicatie systemen baseert op SCA, de nieuwe requirement die specifieke technische standaarden introduceert zoals PSD2-compliant certificaten.

In het uitvoeren van dit onderzoek zal er dus moeten worden gekeken naar welke richtlijnen en eisen van toepassing zijn voor het gecentraliseerde management systeem alsook naar hoe deze kunnen worden geïmplementeerd.

3. Methodologie

Het onderzoek naar centrale truststorebeheer in een banknetwerk zal opgedeeld worden in drie fases: een literatuurstudie, praktijkstudie en uiteindelijke rapportage en oplevering.

In de eerste maand zal de eerste fase van het onderzoek uitgevoerd worden, de literatuurstudie.

Het doel in deze fase is om een diepgaand begrip te krijgen over trust management, certificaatbeheer en de verschillende aanpakken bij truststorebeheer.

In deze literatuurstudie zal er gekeken worden naar de bestaande theorieën, technologieën en andere tools die momenteel worden gebruikt in praktijk.

Ook zal er gekeken worden naar de voordelen van gecentraliseerde truststorebeheer en de eisen binnen de financiële sector.

Op het einde van de eerste fase zal er samen gezeten worden met de co-promotor om mogelijke oplossingen te bespreken die verder zullen worden uitgewerkt in de praktijkstudie.

De info die verkregen wordt in deze literatuurstudie zal de basis leggen voor de volgende fase van dit onderzoek: de praktijkstudie.

Deze fase zou starten in maart en loopt tot eind april met een duur van 8 weken. Deze praktijkstudie opgedeeld in 3 delen.

het ontwerpen van een virtuele omgeving, de implementatie van het centraal truststorebeheer en de evaluatie van de oplossing.

In de eerste stap zal er weer worden samengezeten met de co-promotor om te bepalen welke componenten van het banknetwerk gesimuleerd moeten worden in de virtuele testomgeving.

Hierbij wordt gekeken naar de typische netwerkarchitectuur van een bank, inclusief servers (zoals applicatieservers en webservers), firewalls, proxyservers en verschillende besturingssystemen (zoals Linux en Windows).

Ook wordt er een certificate authority (CA) opgezet om het beheer van certificaten te simuleren.

Deze virtuele omgeving zal worden opgezet binnen GNS3, een netwerkemulator die het mogelijk maakt om complexe netwerken te simuleren.

Het doel is om een realistisch netwerk te creëren dat de complexiteit van een bankomgeving weerspiegelt.

De tweede stap, de implementatie van centraal truststorebeheer, begint midden maart en duurt drie weken.

In deze fase wordt een gecentraliseerde oplossing voor truststorebeheer opgezet. Dit gebeurt door middel van de tools die gekozen werden samen met de co-promotor in de literatuurstudie in combinatie met zelfgeschreven scripts voor het certificaatbeheer.

Het doel hier is dat bij het genereren of updaten van een nieuw root certificaat, de truststores op elk systeem in het netwerk consistent zijn. Ook zullen er veiligheidscontroles geïmplementeerd worden, zoals het monitoren voor ongeldige of verlopen certificaten.

Na de implementatie volgt de derde stap van de praktijkstudie, die bestaat uit de evaluatie en validatie van de oplossing.

Deze fase begint begin april en duurt drie weken.

De centrale vraag is hoever de geïmplementeerde oplossing voldoet aan de beveiligingseisen (zoals DORA, PSD2, GDPR, ISO,...) van een bankennetwerk.

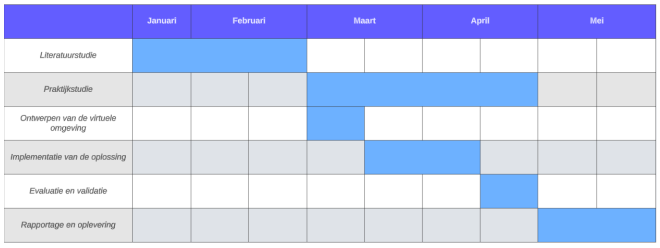
Er worden testcases opgesteld om veelvoorkomende uitdagingen te simuleren, zoals het herroepen van een rootcertificaat of het omgaan met verlopen certificaten.

Ook wordt de schaalbaarheid en efficiëntie van de oplossing getest.

Bij de schaalbaarheid zal er gekeken worden naar hoe de oplossing omgaat met het veranderen of uitbreiden van het netwerk. Bij de efficiëntie zal er gekeken worden naar hoe snel aanpassingen van certificaten binnen de centrale truststore verspreid worden binnen het netwerk zonder het verstoren van andere diensten.

Als laatste fase van dit onderzoek zal er een rapportage gemaakt worden. Dit zal gebeuren in het begin van mei met een tijdsduur van 4 weken. De rapportage zal de ontwerpkeuzes en oplossing beschrijven alsook de evaluatie en resultaten van deze oplossing.

Op basis van de bevindingen worden dan conclusies en aanbevelingen geformuleerd voor de implementatie van centraal truststorebeheer in banknetwerken.



4. Verwacht resultaat, conclusie

Dit onderzoek verwacht dat gecentraliseerd truststorebeheer verbeteringen oplevert in beveiliging, efficiëntie en schaalbaarheid voor een banknetwerk.

Door de certificaten op een centrale plaats te beheren, wordt het risico op verlopen of ongeldige certificaten verkleind, wat de volledige netwerkbeveiliging versterkt.

Het gecentraliseerde beheer zal ook de efficiëntie verhogen door automatisering van certi-

ficaatdistributie, wat tijd bespaart en menselijke fouten vermindert.

Bovendien maakt de oplossing schaalbaarheid mogelijk, wat essentieel is voor de groei van banknetwerken.

Dit onderzoek zal praktische aanbevelingen bieden voor de implementatie van deze oplossing in bankomgevingen, waardoor banken hun certificaatbeheer kunnen optimaliseren en hun netwerkbeveiliging kunnen versterken.

In conclusie verwacht dit onderzoek te bevestigen dat gecentraliseerd truststorebeheer niet alleen de veiligheid verbetert, maar ook bijdraagt aan een efficiënter en beter beheersbaar netwerk, met duidelijke voordelen voor de banksector.

Referenties

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/

Digicert. (2025). What is a digitalcertificate? *Trust PKI*. https://www.digicert.com/faq/trust-and-pki/what-is-a-digital-certificate-and-why-are-digital-certificates-important

Dwivedi, D. (2024). What is a Trust Store and the Issues Associated with It. *Encryption Consulting*. https://www.encryptionconsulting.com/what-is-a-trust-store-and-the-issues-associated-with-it/

Gorobeț, I. (2024). Convergence of banking cybersecurity strategies to the new rules on digital operational resilience. *Proceedings of International Conference "Economic Security in the Context of Systemic Transformations"*. https://doi.org/10.53486/escst2023.06

Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *International Cybersecurity Law Review*, *5*(1), 79–120. https://doi.org/10.1365/s43439-023-00108-8

IBM. (2023, oktober). IBM z/OS Connect. https://www.ibm.com/docs/en/zos-connect/zosconnect/3.0?topic=connect-keystores-truststores

Mervana, P. (2024). What is a Trust Store and How to Manage It? *SSL Insight*. https://sslinsights.com/what-is-trust-store-and-how-to-manage-it/

Topping, S. (2023). Understanding Public Key Infrastructure: Overview and Key Concepts. *GlobalSign Blog*. https://www.globalsign.com/en/blog/understanding-pki-overview-and-key-concepts