**Klant info beveiliging onderzoeks document**

Inhoud

[Introductie 3](#_Toc182570533)

[Hoe beveilig ik de informatie van mijn klanten het beste? 4](#_Toc182570534)

[Welke methoden van informatiebeveiliging zijn er? 4](#_Toc182570535)

[Hoe beveiligen de uitgezochte manieren informatie? 4](#_Toc182570536)

[1. Encryptie (TLS) 4](#_Toc182570537)

[2. Tokenization 5](#_Toc182570538)

[3. Data-at-Rest Encryption (DARE) 6](#_Toc182570539)

[4. PCI-DSS Compliance 6](#_Toc182570540)

[5. Multi-Factor Authentication (MFA) 7](#_Toc182570541)

[Welke manieren van informatiebeveiliging zijn realistisch voor mij om te implementeren? 7](#_Toc182570542)

[Conclusie 8](#_Toc182570543)

[Referenties 9](#_Toc182570544)

# Introductie

Wanneer een klant iets koopt van een web shop zal die adres info moeten invullen zodat het bestelde goed op de correcte locatie geleverd wordt. Om ervoor te zorgen dat de informatie van de klant niet door derde partijen met slechte bedoelingen gebruikt wordt zijn er verschillende beveiliging methodes beschikbaar tijdens het maken van de web shop. In dit document worden er enkele methodes besproken en geconcludeerd met welke methodes ik zal gebruiken in de opzet van mijn web shop.

# Hoe beveilig ik de informatie van mijn klanten het beste?

Om te bepalen welke informatiebeveiligingsmethoden geschikt zijn voor mijn toepassing, moet eerst een overzicht worden gemaakt van de verschillende manieren waarop gebruikersinformatie beveiligd kan worden. In dit document worden de volgende vragen beantwoord:

* **Welke methoden van informatiebeveiliging zijn er?**
* **Hoe beveiligen deze methoden informatie?**
* **Welke methoden zijn voor mij realistisch om te implementeren?**

# Welke methoden van informatiebeveiliging zijn er?

Aangezien er verschillende manieren zijn om gebruikersinformatie te beveiligen, richt dit onderzoek zich op vijf veelgebruikte beveiligingsmethoden. De vijf methoden die besproken worden zijn:

1. **Encryptie (Encryption)**
2. **Tokenisatie (Tokenization)**
3. **Encryptie van data in rust (Data-at-Rest Encryption)**
4. **PCI-DSS compliance**
5. **Multi-Factor Authenticatie (MFA)**

## Hoe beveiligen de uitgezochte manieren informatie?

Om te bepalen welke beveiligingsmethoden het meest geschikt zijn voor mijn project, is het essentieel om te begrijpen hoe deze methoden werken en welke beveiligingslagen zij toevoegen. Hieronder volgt een gedetailleerde beschrijving van de vijf eerder geïdentificeerde beveiligingsmethoden: **Encryptie (TLS), Tokenization, Data-at-Rest Encryption (DARE), PCI-DSS compliance**, en **Multi-Factor Authentication (MFA)**.

## 1. Encryptie (TLS)

Encryptie beschermt gegevens die tussen een client (bijv. een gebruiker op een webshop) en een server worden verzonden via het internet. Het meest gebruikte protocol hiervoor is **TLS (Transport Layer Security)**, dat de oudere **SSL (Secure Sockets Layer)** heeft vervangen. TLS versleutelt de communicatie tussen de client en de server, zodat onbevoegden de gegevens niet kunnen inzien of manipuleren.

**Werking:**

* **Asymmetrische encryptie:** Wordt gebruikt om een beveiligde verbinding op te zetten. Hierbij worden openbare en private sleutels gebruikt om een veilige sessie tot stand te brengen.
* **Symmetrische encryptie:** Zodra de verbinding is gemaakt, wordt symmetrische encryptie gebruikt om gegevens veilig uit te wisselen binnen de sessie.

Om TLS te implementeren, moet een website een **SSL-certificaat** aanschaffen. Dit certificaat biedt de mogelijkheid om TLS te gebruiken en zorgt ervoor dat de verbinding tussen de gebruiker en de server beveiligd is.

**Kosten:** De prijs voor een SSL-certificaat varieert van $60 tot $1000 per jaar, afhankelijk van het type certificaat.

(*What Is SSL/TLS Encryption?, n.d.)*

## 2. Tokenization

**Tokenization** wordt veel gebruikt in betalingssystemen om gevoelige informatie, zoals creditcardgegevens, te beschermen. Hierbij worden gevoelige gegevens vervangen door een willekeurige reeks symbolen (tokens), die geen intrinsieke waarde hebben en niet kunnen worden teruggeconverteerd zonder toegang tot een beveiligde database die de oorspronkelijke gegevens bevat.

**Werking:**

* **Tokens:** De originele gegevens worden omgezet in tokens die geen gevoelige informatie bevatten, maar toch als referentie kunnen dienen in transacties.
* **Blockchain-ledger:** Bij betalingen kan een private blockchain-ledger worden gebruikt om transacties bij te houden, maar zonder de oorspronkelijke gegevens bloot te stellen.

Tokenization beschermt gegevens tijdens het betalingsproces, maar vereist aanvullende systemen voor herstel in geval van diefstal of verlies.

(*What Is Tokenization?, 2024)*

## 3. Data-at-Rest Encryption (DARE)

**Data-at-Rest Encryption (DARE)** is een methode om gegevens te versleutelen terwijl deze zijn opgeslagen op schijven, servers of databases. In tegenstelling tot TLS, dat zich richt op gegevens tijdens de overdracht, beschermt DARE inactieve gegevens tegen toegang door onbevoegden.

**Werking:**

* **Versleuteling van opgeslagen data:** Gegevens worden versleuteld wanneer deze niet actief worden gebruikt of overgedragen, bijvoorbeeld in een database.
* **Toegangscontrole:** Gebruikers krijgen alleen toegang tot gegevens die voor hen relevant zijn, op basis van een hiërarchische beveiliging.

DARE is vooral nuttig voor het beschermen van klantgegevens zoals accountinformatie en persoonlijke details binnen databases. Dit type encryptie garandeert dat zelfs als iemand fysieke toegang krijgt tot de server of database, de gegevens ontoegankelijk blijven zonder de juiste decryptiesleutel.

(*Emptoris Strategic Supply Management 10.1.3, n.d.)*

## 4. PCI-DSS Compliance

**PCI-DSS (Payment Card Industry Data Security Standard)** is een beveiligingsstandaard die is ontworpen om de veiligheid van creditcardgegevens te waarborgen. Organisaties die betalingen verwerken, moeten voldoen aan deze standaard. Dit omvat zowel technische als organisatorische maatregelen om klantgegevens te beschermen.

**Vereisten:**

1. **Veilige overdracht van creditcardgegevens:** Het gebruik van encryptie en veilige communicatiemiddelen om gevoelige gegevens te versturen.
2. **Veilige opslag:** Het waarborgen van de veiligheid van opgeslagen persoonlijke en betalingsgegevens.
3. **Audits en testen:** Jaarlijkse controles en penetratietests om de veiligheid te waarborgen.

Veel websites maken gebruik van derde partijen zoals **Stripe** en **PayPal** om aan PCI-DSS te voldoen, aangezien deze bedrijven gespecialiseerd zijn in de beveiliging van betalingsgegevens.

(*Wat Is PCI DSS-compliance? 12 Vereisten | Stripe, n.d.)*

## 5. Multi-Factor Authentication (MFA)

**Multi-Factor Authentication (MFA)** is een authenticatiemethode die meerdere stappen vereist om toegang te krijgen tot een account of service. Deze methode combineert iets dat de gebruiker weet (zoals een wachtwoord) met iets dat de gebruiker bezit (zoals een telefoon of authenticatie-app).

**Werking:**

* **Meerdere verificatiestappen:** Na het invoeren van een gebruikersnaam en wachtwoord, moet de gebruiker bijvoorbeeld een eenmalige code invoeren die naar zijn telefoon wordt gestuurd.
* **Extra beveiligingslaag:** Zelfs als een wachtwoord wordt gestolen, is toegang niet mogelijk zonder de aanvullende verificatiestap.

MFA voegt een extra beveiligingslaag toe om te voorkomen dat onbevoegden toegang krijgen tot accounts, zelfs als de gebruikersnaam en het wachtwoord zijn gestolen.

(*Versterk Uw IT-beveiliging Met Multi-Factor Authenticatie (MFA)!, 2024)*

## Welke manieren van informatiebeveiliging zijn realistisch voor mij om te implementeren?

Omdat PCI-DSS Compliance gaat over meerdere regels sommige waarvan de eis stellen van het implementeren van de andere methodes die ik in dit document onderzocht heb is dit de minst realistische methoden om als individu te implementeren voor het beveiligen van klanten informatie.

Daarbuiten zijn er twee methodes die realistisch zijn voor mij om tee implementeren. Deze methodes zijn encryptie (TLS) en Multi-factor authenticatie. Deze methodes zijn zo simpel om te implementeren op een basis level dat ik van plan ben beide te implementeren in mijn websiteapplicatie het resultaat daarvan zal ik documenteren in een verder stuk van dit document.

# Conclusie

Voor mijn individueel project ga ik gebruik maken van encryptie (TLS) en Multi-factor authenticatie om de info van mijn klanten veilig en buiten bereik van derde partijen te houden.

# Referenties

*What is SSL/TLS Encryption?* (n.d.). F5, Inc. <https://www.f5.com/glossary/ssl-tls-encryption>

G, M. (2024, July 1). *SSL certificate cost in 2024: How much to spend on an SSL certificate*. Hostinger Tutorials. <https://www.hostinger.com/tutorials/ssl-certificate-cost>

*What is tokenization?* (2024, July 25). McKinsey & Company. <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-tokenization>

*Emptoris Strategic Supply Management 10.1.3*. (n.d.). <https://www.ibm.com/docs/en/strategicsm/10.1.3?topic=security-data-rest-encryption>

*Wat is PCI DSS-compliance? 12 vereisten | Stripe*. (n.d.). <https://stripe.com/nl/guides/pci-compliance>

*Versterk uw IT-beveiliging met Multi-Factor Authenticatie (MFA)!* (2024, June 20). Identity Management | Tools4ever. <https://www.tools4ever.nl/kennisbank/multi-factor-authenticatie-mfa/>