///Encryptie en sleutelbeheer (PKI)

1 INTRODUCTIE

Als lokaal bestuur speelt de beveiliging van informatie een cruciale rol. Encryptie, een krachtige techniek die gegevens omzet in een onleesbare vorm, biedt een essentiële buffer tegen ongeautoriseerde toegang. Het is de basis van moderne beveiliging en maakt veilige communicatie mogelijk in een tijdperk waar gevoelige informatie constant wordt uitgewisseld.

Binnen encryptie zijn er twee hoofdzaken: symmetrische encryptie, waarbij dezelfde sleutel wordt gebruikt voor zowel versleuteling als ontsleuteling en asymmetrische-encryptie, waarbij er gebruik wordt gemaakt van twee sleutels – één openbare sleutel (public key) en één privésleutel (private key) voor ontsleuteling. De private key is enkel bestemd voor de eigenaar van de informatie en moet daarom goed beveiligd worden. De versleutel methode die gebruik maakt van twee sleutels, bekend als Public Key Infrastructure (PKI), heeft de manier waarop we digitale veiligheid benaderen veranderd.

Public Key Infrastructure (PKI) biedt een robuust kader voor het beheer van sleutels en digitale certificaten waardoor veilige communicatie tussen bijvoorbeeld burgers en een lokaal bestuur mogelijk is zonder voorafgaande uitwisseling van geheime sleutels. Met behulp van Public Key Infrastructure (PKI) kunnen gebruikers hun identiteit digitaal bevestigen, data ondertekenen en versleutelen veilige online transacties uitvoeren.

2 HOE VERLOOPT VERSLEUTELING?

Er bestaan meerdere soorten encryptie: symmetrische en asymmetrische encryptie. Elk van deze methoden heeft unieke eigenschappen en toepassingen in de wereld van digitale beveiliging. Denk bijvoorbeeld maar aan het versturen van e-mail, bestanden of volledige netwerken (VPN).

Bij symmetrische encryptie wordt hetzelfde wachtwoord gebruikt voor zowel het versleutelen als het ontsleutelen van gegevens. Aangezien dezelfde sleutel wordt toepast aan beide zijden van de communicatie, staat dit proces bekend om zijn eenvoud en efficiëntie. Symmetrische encryptie wordt vaak gebruikt bij het opslaan van documentatie of het beveiligen van bestanden waarbij snelheid en minimale rekenkracht essentieel zijn.

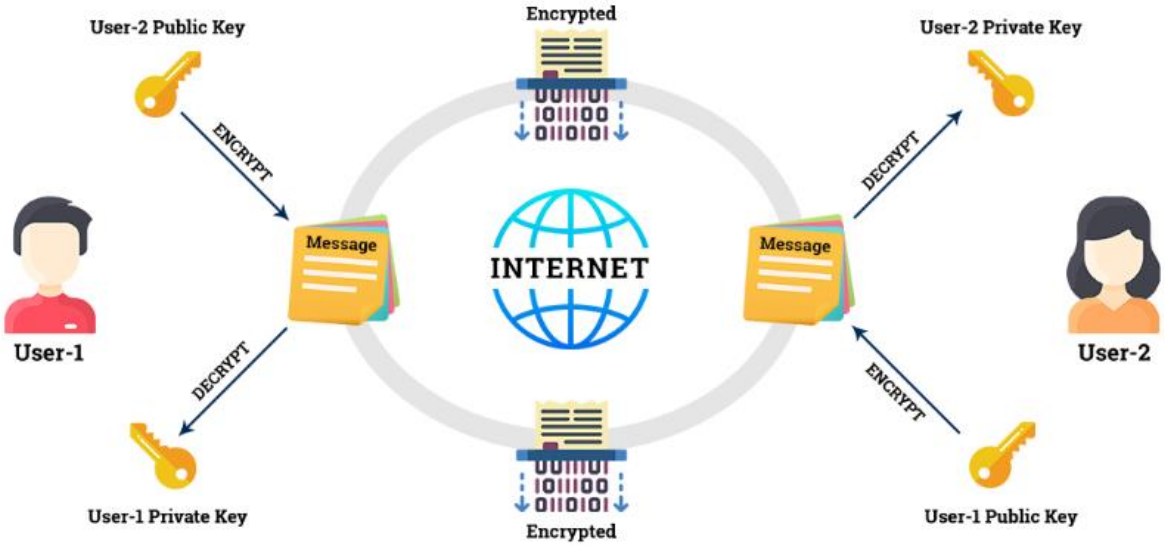
Bij asymmetrische encryptie wordt gebruik gemaakt van twee sleutels: een publieke sleutel en een private sleutel. De publieke sleutel fungeert als een mechanisme voor veilige communicatie en identiteitsverficatie.

Ten eerste maakt versleuteling met de publieke sleutel het mogelijk om gegevens veilig te versturen. Alleen de bezitter van de bijhorende private sleutel kan deze versleutelde gegevens ontsleutelen, wat de vertrouwelijkheid garandeert.

Ten tweede wordt de publieke sleutel gebruikt voor het verifiëren van digitale handtekeningen, gemaakt met de bijhorende private sleutel. Hierdoor kan men zeker zijn van de integriteit en authenticiteit van de ontvangen gegevens.

Hieronder vindt u de stappen die genomen worden bij asymmetrische encryptie:

1. **Sleutelpaar genereren:**
    - De ontvanger genereert een sleutelpaar bestaande uit een publieke sleutel en een bijbehorende private sleutel.
2. **Publieke sleutel verspreiden:**
    - De ontvanger verspreidt de publieke sleutel naar iedereen die versleutelde berichten naar hen wil sturen. De publieke sleutel kan veilig worden gedeeld omdat het- in tegenstelling tot de private sleutel- geen gevoelige informatie onthult.
3. **Versleutelen van gegevens:**
    - De verzender verkrijgt de publieke sleutel van de ontvanger en gebruikt deze om gegevens te versleutelen. Dit versleutelde bericht kan alleen worden ontsleuteld door de ontvanger met behulp van hun eigen bijbehorende private sleutel.
4. **Verzenden van versleutelde gegevens:**
    - De verzender stuurt het versleutelde bericht naar de ontvanger. Omdat alleen de ontvanger beschikt over de bijbehorende private sleutel, kan deze de versleutelde gegevens decoderen.
5. **Decryptie van gegevens:**
    - De ontvanger gebruikt hun eigen private sleutel om de ontvangen versleutelde gegevens te ontsleutelen en het originele bericht te herstellen.
6. **Digitale handtekening genereren:**
    - Als de verzender een digitale handtekening wil toevoegen aan het bericht, gebruikt deze zijn of haar private sleutel om een unieke digitale handtekening te genereren. Deze handtekening wordt vaak gecreëerd door een hash van het bericht te versleutelen met de private sleutel.
7. **Verzenden van het ondertekende bericht:**
    - De verzender stuurt het originele bericht samen met de digitale handtekening naar de ontvanger.
8. **Verificatie van digitale handtekening:**
    - De ontvanger gebruikt de publieke sleutel van de verzender om de digitale handtekening te verifiëren. Als de handtekening geldig is, kan de ontvanger er zeker van zijn dat het bericht afkomstig is van de verzender en dat het niet is gewijzigd tijdens de overdracht.



Bron: https://www.ssl2buy.com/cybersecurity/pki-public-key-infrastructure-management

3 AANBEVELINGEN

Hieronder vindt u een aantal aanbevelingen die het Cyber Response Team voor Lokale Besturen (Vo-CRT) geeft met betrekking tot (het implementeren) van een Public Key Infrastructure (PKI).

Organisatorische maatregelen

- Stel een duidelijk en gedocumenteerd informatieveiligheidsbeleid op dat de richtlijnen en verwachtingen voor alle medewerkers definieert.
- Implementeer een strikt toegangsbeheerbeleid om ervoor te zorgen dat medewerkers alleen toegang hebben tot de informatie en middelen die relevant zijn voor hun functie.
- Ontwikkel en oefen een gedetailleerd incident responseplan, zodat het personeel snel en effectief kan reageren op beveilig incidenten.
- Werk alleen samen met een vertrouwde en goede certificate authority (CA) om de integriteit van digitale certificaten te waarborgen.
- Implementeer een sleutelbeheerbeleid dat de veilige generatie, distributie, opslag en rotatie van sleutels regelt.
- Implementeer uitgebreide audit logs en monitoringsmechanismen om activiteiten met betrekking tot digitale certificaten en sleutel bij te houden.

Technische maatregelen

- Gebruik sterke en up-to-date cryptografische algoritmen voor sleutelgeneratie, versleuteling en ondertekening van digitale certificaten.
- Maak gebruik van beveiligde opslag voor private sleutels.

- Zorg ervoor dat digitale certificaten tijdig worden gevalideerd en geverifieerd. Dit omvat het controleren van de handtekening en het verifiëren van de geldigheid van het certificaat.
- Implementeer Multi-Factor Authenticatie (MFA) om een extra laag beveiliging toe te voegen aan gebruikersauthenticatie.
- Splits het netwerk op in segmenten om de verspreiding van aanvallen te beperken en het beheer van beveiligingsbeleid te vereenvoudigen.

Mensgerichte maatregelen

- Organiseer voldoende kennistrainingen voor IT-medewerkers.
- Het belang benadrukken van Public Key Infrastructure (PKI) binnen een lokaal bestuur.

4 VERKLARENDE WOORDENLIJST

Verklarende woordenlijst

Term	Verduidelijking	Link naar meer informatie
VPN	Virtual Private Network is een beveiligde verbinding die je online activiteiten versleutelt en je internetverkeer via een externe server leidt, waardoor je privacy veiligheid worden vergroot door je echte IP-adres te verbergen.	https://consumentenbond.nl/veilig-internetten/veiliger-internetten-met-een-vpn
Hash	Een hash is een output die wordt gegenereerd door een hashfunctie, waarbij inputgegevens van willekeurige grootte worden omgezet in vaste, unieke reeks tekens. Het wordt gebruikt voor het beveiligen van gegevensintegriteit en wachtwoordopslag, omdat zelfs kleine wijzigingen in de input een compleet andere hash opleveren.	https://www.techtarget.com/searchdatamanagement/definition/hashing
CA	Certificate Authority (CA) is een vertrouwde entiteit die digitale certificaten uitgeeft en ondertekent om de authenticiteit van de openbare sleutel van een gebruiker, server of apparaat te waarborgen. Hierdoor kunnen andere veilig communiceren met de entiteit en de geldigheid van de versterkte certificaten verifiëren.	https://www.ssl.com/faqs/what-is-a-certificate-authority/
MFA	Multi-Factor Authenticatie is een beveiligingsmethode waarbij gebruikers hun identiteit bevestigen door meer dan één verificatiemiddel te gebruiken, zoals een wachtwoord in combinatie met een verificatiecode via een mobiele app. Dit verhoogt de beveiliging door meerdere lagen van authenticatie te vereisen voor toegang tot systemen of gegevens.	https://www.vlaanderen.be/digitaal-vlaanderen/toegangsbeheer

5 REFERENTIES

- Minimale IAM-maatregelen Vlaamse Overheid:

https://assets.vlaanderen.be/image/upload/v1663779254/Vo_Informatieclassificatie_-_Minimale_maatregelen_-_IAM_xle0xg.pdf