UWV

UWV ICT Richtlijn Cryptografische beheersmaatregelen (versleuteling)

werken aan perspectief

Bestandsnaam	UWV ICT 20200804_Richtlijn Cryptografische Beheersmaatregelen V2.Docx
Versie	2.0
Datum	04-08-2020

Opdrachtgever	Eigenaar
Naam: Alex Kooistra	André van Alphen
Functie: Chief Information Security Officer (CISO)/	dir ICT-Services
Datum akkoord:04-08-2020	04-08-2020

Auteur

Naam: Kato Vierbergen

Functie: Information Security Officer, CISO-office

Versie: 2.0

Inhoud

Versiebeheer

Versie	Datum	Wijzigingen	Distributie	Besluit
0.1	27-02-2015	1ste concept		Ter review aanbieden aan team
0.2	20-03-2015	2de concept	Ter review aangeboden aan projectteam	Ter review aanbieden aan stakeholders
0.3	30-03-2015	Commentaar team verwerkt.	ICT-security, IS infrastructuur, AD, K&S, Werkbedrijf	Ter review aanbieden aan C-IB&P en PTO
0.4	15-05-2015	Commentaar ICT-security, IS infrastructuur, AD, K&S en Werkbedrijf verwerkt en akkoord verkregen.	Coördinatoren IB&P	Verwerken commentaar
0.5	25-06-2015	Commentaar Coördinatoren IB&P verwerkt en akkoord verkregen.	PTO	Ter goedkeuring aanbieden aan coalitie IB&P tactisch
0.9			Ter goedkeuring stuurgroep GoIB	Akkoord
0.91	28-12-2015	Commentaar AB	IV-Team	Akkoord
1.0	28-12-2015		Instemming IV-Team	Akkoord
1.9	30-08-2018	Review 2018 - upgrade van versie 1.0 n.a.v. nieuwe wetgeving o.a. AVG. Afgesproken is dat alle richtlijnen updates n.a.v. AVG na half jaar worden evalueert op impact. Een versie 2.0 wordt daarna vastgesteld!	Ingebracht 02/08. Terugkoppeling 16/08. Instemming/vaststellen 30/08 AB+	Akkoord
1.9		Idem	Ingebracht 17-07 opnieuw 16/08, review 28/08, instemming 20/09 IB&P Tactische Coalitie	Loopt voor instemming.
1.9	01-10-2018	Idem	DT C-ICT vaststelling	
1.9	30-10-2018	Idem	IV Team vaststelling	instemming
2.0	11-12-2019	Richtlijn Cryptografische beheersmaatregelen, losgeknipt van Cryptografiebeleid UWV en hernoemd in opvolging van de BIO.	AB+, TC ter review	
2.0	25-06-2020	Richtlijn Cryptografische beheersmaatregelen, reviewcommentaren verwerkt	AB+ en TC, Ter instemming verwerking reviewcommentaren	instemming
2.0	03-07-2020	Richtlijn Cryptografische beheersmaatregelen	FG voor instemming op borging AVG	instemming
2.0	04-08-2020		IV-Board voor vaststelling en overdracht aan Eigenaar ICT-Services	vastgesteld

Noot:
Deze richtlijn wordt elk jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. Dit is o.a. aan de orde wanneer wetgeving, verordeningen e.d. ten aanzien van informatiebeveiliging wordt of is uitgebracht.
De CISO is opdrachtgever voor dit document. ICT-services is eigenaar van dit document.

Dit document is de **Richtlijn Cryptografische beheersmaatregelen UWV versie 2.0**
In lijn met de BIO is in 2019 bij de vorming van de versie 2.0 de Richtlijn Encryptie hernoemd naar Richtlijn Cryptografische beheersmaatregelen. Daarbij is deze tevens onderverdeeld in 2 delen: Cryptografiebeleid UWV v 2.0 en de Richtlijn Cryptografische beheersmaatregelen v2.0. (Binnen de cryptografie is encryptie een van de maatregelen, wat staat voor het coderen (versleutelen) van gegevens op basis van een bepaald algoritme.)

1. Inleiding

1.1. Doel

Het doel van deze Richtlijn Cryptografische beheersmaatregelen is nader invulling geven aan het Cryptografiebeleid UWV. Cryptografische beheersmaatregelen zijn belangrijke hulpmiddelen om als risico mitigerende maatregel in te kunnen zetten voor de bescherming van de bedrijfsgegevens en de persoonsgegevens. Het doel van cryptografische beheersmaatregelen is te zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, integriteit van informatie en authenticiteit van de afzender te borgen.

1.2. Doelgroep

Dit document is van belang voor partijen, (mede)verantwoordelijk voor de veiligheid van informatie. De richtlijn Cryptografische beheersmaatregelen is een uitwerking van het Cryptografiebeleid UWV en bevat voornamelijk technische maatregelen om beveiligingsrisico's te mitigeren. Het is bedoeld voor UWV functionarissen die informatiebeveiliging in de ontwerpen mee moeten nemen. Daarnaast is het ook voor ICT-beheer bedoeld, die deze cryptografische beheersmaatregelen moet gaan beheren.

1.3. Leeswijzer

In deze Richtlijnen Cryptografische beheersmaatregelen worden de hoofdnomen nader uitgewerkt en passende standaarden en maatregelen aangereikt.

Cryptografische beheersmaatregelen hebben over het algemeen een grote invloed op de ICT technische infrastructuur, systemen en devices. Informatie in bijlage A kan helpen bij het wegen van de te maken keuzes voor inzet van cryptografische beheersmaatregelen als risico mitigerende maatregelen. Deze informatie is niet bindend.

Voorafgaande aan het toepassen van cryptografische beheersmaatregelen is een risicoafweging (RA) en/of een Gegevensbeschermingseffectbeoordeling (GEB) noodzakelijk, zodat in de Project Start Architectuur (PSA) meegewogen wordt in hoeverre de beveiligings- en privacyrisico's al gemitigeerd worden, bijvoorbeeld door:

I. anonimiseren.
II. pseudonimiseren (AVG art. 4 lid 5).
III. En het toepassen van dataminimalisatie (AVG art. 5 lid 1 sub C).

De richtlijnen voor toepassen van cryptografische beheersmaatregelen zijn verdeeld naar:

A. algemene regels
B. specifieke regels
    1. Gegevensuitwisseling via web portalen / Mobiele Apps;
    2. Gegevensuitwisseling tussen UWV- en externe applicaties;
    3. Gegevens in opslag;
    4. Gebruik gegevens intern UWV;
    5. Beleidsregels voor de beheer organisatie.

1.4. De scope

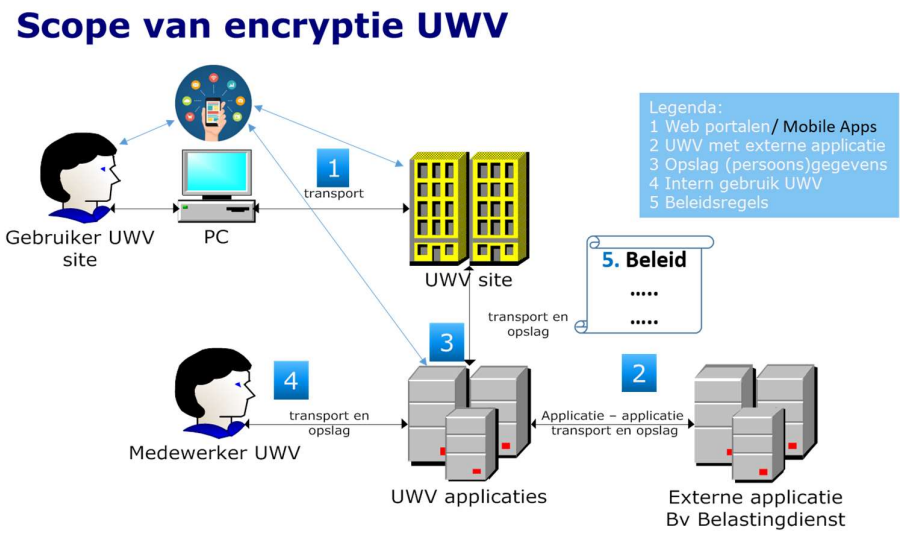


Fig 1: Scope (hoog over) van cryptografische beheersmaatregelen als technisch risico mitigerende maatregel.

Voor het bepalen van het toepassingsgebied van cryptografische beheersmaatregelen maken we onderscheid in:

- Binnen het UWV-datacenter of in verbinding met buiten het UWV-datacenter
- Gegevenstoestand: 'in use', 'in transit' of 'at rest'

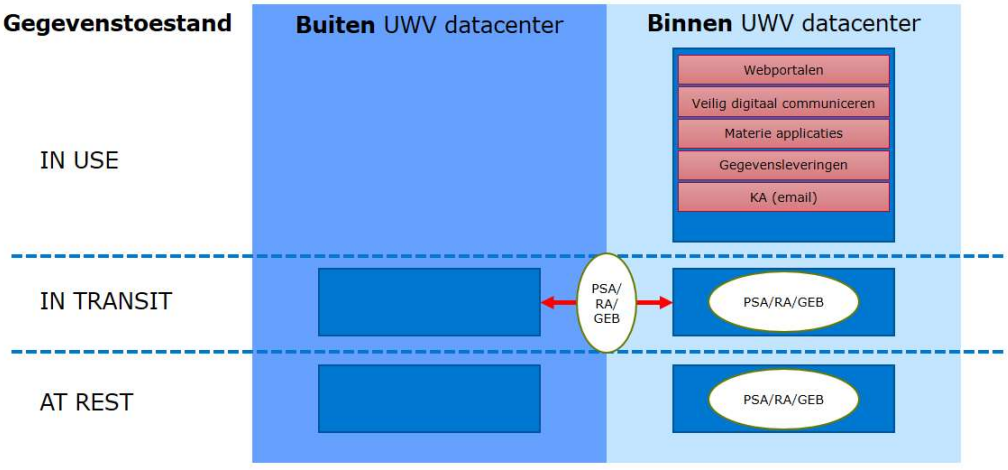


Fig 2: scope in relatie tot gegevenstoestand

De feitelijke cryptografische beheersmaatregelen worden bij iedere wijziging opnieuw bepaald en vastgelegd in de Project Start Architectuur (PSA), de RisicoAnalyse (RA) en wanneer er persoonsgegevens verwerkt worden ook in de Gegevensbeschermingseffectbeoordeling (GEB)

2. Criteria en cryptografische beheersmaatregelen

In de volgende paragrafen worden de eisen en maatregelen voor cryptografische beheersmaatregelen uit de BIR in SIVA termen beschreven.

Bij toepassing moet deze set eisen en maatregelen context en techniek afhankelijk uitgewerkt worden, in lijn met deze richtlijn cryptografische beheersmaatregelen, in inrichtingseisen met als eindresultaat een set eenduidig meetbare eisen.

Toelichting beschrijving criteria en maatregelen in SIVA-syntax

Per criterium wordt in dit hoofdstuk kort aangegeven wat de onderbouwing voor de norm is, met een voorstel voor de te implementeren maatregelen. Bij de beschrijving wordt gebruik gemaakt van het SIVA-raamwerk. Dit bevat vier componenten:

- **S**tructuur;
- **I**nhoud;
- **V**orm;
- **A**nalyse.

De opbouw per beveiligingseis is in de SIVA-syntax, namelijk:

Context

Een beschrijving van het mechanisme.

Na de contextbeschrijving volgt de template voor het beschrijven van een hoofdcriterium en de onderliggende sub criteria.

Criterium X De Naam van het criterium.		
Criterium	De norm, namelijk '**wie**' en '**wat**'. Het criterium is gelijk aan de norm / architectuurprincipe.	Referenties andere normen-kaders
	Wie xxxxx Wat xxxx trefwoord xxx	
Doelstelling	Het gewenste resultaat, namelijk '**waarom**'.	
Risico	Een beschrijving van mogelijk misbruik of schade.	

Maatregelen (of indicatoren)

ISOR ID[1] - Trefwoord: Maatregelenreferentie (of Indicatorreferentie)		
Maatregeln r.	De mogelijke maatregelen, namelijk het '**hoe**'. De maatregelen of indicatoren zijn de principle driven rules waaraan invulling wordt gegeven om te voldoen aan het criterium.	Referenties andere normen-kaders

[1] De ISOR-aanduiding van de criteria wordt toegelicht op deze NORA-pagina en verwijst naar een Beleids- (BE), Uitvoerings-(UE) of Control (CE)-criterium: https://www.noraonline.nl/wiki/Uitleg_ID_binnen_ISOR

Bij de referenties wordt, voor zover relevant, aangegeven waar in de volgende standaarden en richtlijnen additionele informatie is te vinden, zoals:

I. UWV BIR, 'Baseline Informatiebeveiliging Rijksdienst', Versie 1.0, 8 december 2014. De UWV BIR is gelijk aan de Rijksbrede BIR van 1 december 2012 met uitzondering van enkele (R)-maatregelen die specifiek op de Rijksdienst zijn gericht. Daar waar deze niet aansluiten bij de UWV-situatie zijn deze aangepast naar de situatie van UWV;
II. ISO27002, 'NEN-ISO/IEC 27002 Code voor informatiebeveiliging', 2005.

Normen en cryptografische beheersmaatregelen in SIVA-syntax

BE 01 Formuleren Cryptografisch beleid		
Criterium	De CIO heeft eisen geformuleerd die worden gesteld aan processen en procedures rond het beheer van cryptografisch materiaal en de opslag en distributie van dit materiaal.	BIR 12.3.2 NCSC B04 Richtsnoer CBP
Doelstelling	Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie/vertrouwelijkheids classificatie).	
Risico	Het beheer van de cryptografische sleutels sluit niet aan bij het beschermingsbelang van de beschermde gegevens, waardoor het beheer van de cryptografische sleutels niet doelmatig is.	

Maatregelen

Processen en procedures		
01	De sleutelbeheer processen zijn in samenhang ingericht. *Zorg daarbij voor processen voor:* a. Sleutel/certificaatgeneratie; b. Sleutel/certificaatdistributie; c. Sleutel/certificaatopslag; d. Sleutel/certificaathernieuwing; e. Sleutel/certificaatherroeping; f. Sleutel/certificaatherstel; g. Sleutel/certificaatarchivering; h. Sleutel/certificaatvernietiging.	BIR 12.3.2 .2 en .4 NCSC B04.01 Richtsnoer CBP
02	Er zijn eisen beschreven voor procedures voor beheer om te zorgen voor een "soepele" migratie wanneer een patch een certificaat van de lijst met vertrouwde certificaten verwijdert.	NCSC B04.02
Opslag en distributie		
03	Er zijn eisen aan opslag van sleutelmateriaal.	NCSC B04.03
04	Er zijn eisen aan distributie van sleutelmateriaal.	NCSC B04.04

Toelichting

01

Zie NIST SP800-57 (deel2)27 en NIST 800-13328 voor standaarden voor cryptografische processen en procedures.

Certificaten hebben een bepaalde geldigheid. Borg dat certificaten tijdig worden vernieuwd. Door het certificaat tijdig te vernieuwen voorkom je onbeschikbaarheid van dienstverlening en blijft de organisatie in staat aan te sluiten bij het vertrouwelijkheidsniveau binnen het PKIoverheid-stelsel.

02

Dit geldt ook als leveranciers een deel van de eerder door hen uitgegeven certificaten intrekt. De maatregelen moeten (langdurige) verstoring van de dienstverlening voorkomen. Dit kan betekenen dat deze patches moeten worden uitgesteld als nog niet alle certificaten van de systemen vervangen zijn.

03

Besteed expliciet ook aandacht aan back-ups met sleutelmateriaal erin.
Zie NIST SP 800-57 (deel 130 en 331) voor standaarden voor het werken met cryptografische technieken en sleutels.
Overweeg bij bedrijf kritische systemen met een hoog beschermingsbelang van de beschermde gegevens een voorschrift voor het gebruik van een hardware security module (HSM).

Hardware Security module (HSM) is een fysiek apparaat dat beschermt en beheert de digitale sleutels voor sterke authenticatie en biedt cryptoprocessing. Deze modules komen traditioneel in de vorm van een plug-in kaart of een extern apparaat dat rechtstreeks aan in computer of een netwerkserver wordt ingebouwd of er wordt aan gekoppeld.

04

Het distribueren van sleutelmateriaal zal minstens zo goed beveiligd moeten zijn als de bescherming die de sleutels moeten leveren.

BE 02 Transactiebeleid formuleren		
Criterium	De CISO formuleert de criteria om vanuit bedrijfs- of procesbelang de integriteit en vertrouwelijkheid van de inhoud van gegevensuitwisseling alsmede de onweerlegbaarheid van een transactie te garanderen.	NCSC B05 SSD-15
Doelstelling	Verantwoording af kunnen leggen over uitgewisselde gegevens, doorgevoerde mutaties en geleverde gegevens.	
Risico	Aansprakelijk gehouden worden voor niet-terechte mutaties of gegevensleveringen terwijl een andere partij verantwoordelijk is.	

Maatregelen

Eisen voor onweerlegbaarheid		
01	Er zijn eisen gesteld aan de (cryptografische) technieken ten behoeve van onweerlegbaarheid die al tijdens de transactie moet worden gewaarborgd.	NCSC B05.02 SSD-13
Eisen voor integriteit en vertrouwelijkheid		
02	Er is een schema voor classificatie van gegevensleveringen/transacties aanwezig.	NCSC B05.01

	Classificatieschema met versleutelingstypes: Alle gegevens, anders dan met Vertrouwelijkheidsklasse 0, worden versleuteld conform beveiligingseisen in de informatiebeveiligingsarchitectuur: a. Vertrouwelijkheidsklasse 1: transportbeveiliging buiten het interne netwerk b. Vertrouwelijkheidsklasse 2: transportbeveiliging [2] c. Vertrouwelijkheidsklasse 3: transport- en berichtbeveiliging	
03	Er is een voorschrift voor het beveiligd opslaan van vertrouwelijke gegevens.	NCSC B05.03
04	Er is een voorschrift voor het beveiligd uitwisselen van vertrouwelijke gegevens.	NCSC B05.04
05	Vertrouwelijke gegevens in databases en bestanden zijn versleuteld of gehashed	NCSC U/WA 05.01
06	Om de integriteit te waarborgen is hashen nodig.	NCSC-TLS

Toelichting

01

Onweerlegbaarheid moet al tijdens de transactie worden gewaarborgd. UWV gebruikt daarvoor de digitale handtekening d.m.v. het gebruik van PKI-overheid certificaten.

02

Hanteer de UWV Richtlijn Classificatie (CDO) en het UWV BIV-beleid[3] (BZ) voor het vaststellen van de vertrouwelijkheidsklasse van de gegevens.

04

Dit is een minimum vereiste. Overweeg om alle informatie via een beveiligde verbinding (zoals TLS) uit te wisselen. Dit heeft als voordeel dat het deel van de communicatie waarin vertrouwelijke gegevens worden uitgewisseld van de buitenkant niet te herkennen is.

05

Soms kan volstaan worden met het versleutelen van enkele tabellen en zelfs kolommen uit tabellen. Dan is het niet nodig een complete database te versleutelen.
Versleuteld opgeslagen gegevens kunnen tijdens communicatie versleuteld blijven, ook wanneer het communicatiekanaal zelf versleuteld is. Dit levert een extra beveiligingslaag mits ze beide met andere sleutels encrypted zijn.

BE 03 Verantwoordelijkheden sleutel/certificaatbeheer organisatie		
Criterium	De taken, verantwoordelijkheden en bevoegdheden van de actoren in de sleutel / certificaatbeheer organisatie moeten zijn beschreven.	BIR 12.3.2
Doelstelling	Een beschrijving van TVB's voor sleutel/certificaatbeheer organisatie schept duidelijkheid in de uitvoering van het beheerproces.	

[2] BIV-beleid: Ten tijde van deze Richtlijn Cryptografische Beheersmaatregelen was het UWV BIV-beleid in bewerking. Hierin wordt ook een Vertrouwelijkheidsklasse 2+ onderscheiden. Zodra dit beleid vastgesteld is, zal deze Richtlijn hierop aangepast worden.

[3] BIV-beleid: Ten tijde van deze Richtlijn Cryptografische Beheersmaatregelen was het UWV BIV-beleid in bewerking. De UWV Richtlijn classificatie zal opgenomen worden in het UWV BIV-beleid.

Risico	Onduidelijkheden in TVB's kunnen leiden tot fouten in het sleutelbeheer waardoor er risico's ontstaan voor de vertrouwelijkheid, integriteit en controleerbaarheid van UWV gegevens.	

Maatregelen

Taken, verantwoordelijkheden en bevoegdheden sleutelbeheer		
01	De TVB van functionarissen en organisatieonderdelen die een rol spelen bij sleutelbeheer zijn beschreven. Functionarissen a. CIO b. CISO Organisatieonderdelen c. Bedrijfsonderdelen d. Infrastructuur Ontwikkeling en Regie e. Juridische zaken f. K&S g. Leveranciersmanagement h. Lijnmanagement i. Security ICT j. Test Service Center	BIR 12.3.2.1

Toelichting

01

De TVB's van genoemde functionarissen en onderdelen zijn beschreven in het Cryptografiebeleid.

BE 04 sleutel/certificaatbeheer		
Criterium	Er zijn eisen voor sleutel/certificaatbeheer vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.	BIR 12.3
Doelstelling	Beschermen van de vertrouwelijkheid of integriteit van informatie, of authenticiteit van de afzender met behulp van cryptografische middelen.	
Risico	Onjuist sleutel/certificaatbeheer vormt een risico voor de vertrouwelijkheid, integriteit of authenticiteit.	

Maatregelen

Eisen voor sleutelbeheer		
01	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.	BIR 12.3.1.1

02	Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen.	BIR 12.3.1.2
03	(R) De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals Federal Information Processing Standard Publication 140-2 (FIPS 140-2) en waar mogelijk het Nationaal Bureau voor Verbindingsbeveiliging (NBV).	BIR 12.3.1.3 Richtsnoer CBP
04	De geldigheidsduur van cryptografische sleutels wordt bepaald aan de hand van de beoogde toepassing en is vastgelegd in het cryptografisch beleid.	BIR 12.3.2.2
05	De vertrouwelijkheid van cryptografische sleutels wordt gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.	BIR 12.3.2.3
06	Er is een procedure vastgesteld waarin is bepaald hoe wordt omgegaan met gecompromitteerde sleutels.	BIR 12.3.2.4
07	(R) Sleutelmanagement is ingericht volgens PKI Overheid.	BIR 12.3.2.5
08	Controle van systeemgebruik. Handelingen van beveiligingsbeheer, zoals de uitgifte en intrekken van cryptosleutels.	BIR 10.2.2.1

BE 05 Beveiligde inlogprocedure		
Criterium	Toegang tot de IT-middelen wordt beheerst met een beveiligde inlogprocedure die aansluit bij het belang van het bedrijfsproces.	BIR 11.5.1
Doelstelling	Voorkomen dat ongeautoriseerden toegang krijgen tot bedrijfsinformatie en informatiesystemen.	
Risico	Misbruik en verlies van vertrouwelijke inloggegevens tijdens het inlogproces en daarmee ongeautoriseerde toegang tot IT-middelen en gegevens.	

Maatregelen

Belang van het bedrijfsproces		
01	Toegang tot besturingssystemen, kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.	BIR 11.5.1.1
02	De inloggegevens worden tegen afluisteren beschermd door gebruik van geschikte cryptografische beheersmaatregelen, gegeven de stand der techniek.	

UE 06 Diensten voor elektronische berichtenuitwisseling en e-commerce		
Criterium	Informatie wordt bij elektronische berichtenuitwisseling en online transacties beschermd.	BIR 10.6.1, 10.8.4, 10.9.2

		NCSC U/WA 05.02 Richtsnoer CBP SSD-2
Doelstelling	De beveiliging bewerkstellingen bij elektronische berichtenuitwisseling en van online transacties en het veilig gebruik van deze diensten.	
Risico	Onvoldoende bescherming tijdens berichtenuitwisseling en online transacties leidt tot risico's voor de vertrouwelijkheid, integriteit en onweerlegbaarheid van de inhoud van daarvan.	

Maatregelen

Informatie wordt beschermd		
01	(R) Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken, zoals het internet, dient altijd geschikte cryptografische beheersmaatregelen te worden toegepast. Zie hiertoe ook 12.3.1.3.	BIR 10.6.1.3 Richtsnoer CBP NSCS U/WA 05.03 SSD-4
02	(R) Digitale documenten binnen UWV waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van PKI Overheid.	BIR 10.8.4.1
03	Een online transactie wordt bevestigd door een (gekwalificeerde) elektronische handtekening of een andere wilsuiting (bijv. een TAN code) van de gebruiker.	BIR 10.9.2.1 NSCS U/WA 05.04
04	Een online transactie is versleuteld, de partijen zijn geauthentiseerd en de privacy van betrokken partijen is gewaarborgd.	BIR 10.9.2.2 Richtsnoer CBP
05	Cookies met vertrouwelijke gegevens zijn versleuteld	NSCS U/WA 05.02 SSD-2

UE 07 Draagbare computers en telewerken		
Criterium	Er zijn geschikte beveiligingsmaatregelen getroffen ter bescherming tegen risico's van het gebruik van draagbare computers.	BIR 11.7.1
Doelstelling	Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers.	
Risico	Onvoldoende beveiliging kan bij verlies of diefstal leiden tot openbaar worden van vertrouwelijke UWV informatie.	

Maatregelen

Beveiligingsmaatregelen		
01	(R) Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van de gegevens conform classificatie-eisen.	BIR 11.7.1.1 Richtsnoer CBP

CE 08 Naleving van wettelijke voorschriften		
Criterium	Cryptografische beheersmaatregelen worden overeenkomstig alle overeenkomsten, wetten en voorschriften gebruikt.	BIR 15.1.6
Doelstelling	Voorkomen van schending van enige wetgeving, wettelijke of regelgevende of contractuele verplichtingen, en van enige beveiligingseisen	
Risico	Schenden van wet- en regelgeving kan leiden tot imago schade voor en/of juridische procedures tegen UWV.	

Maatregelen

Overeenkomsten, wetten en voorschriften		
01	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften het gebruik van cryptografische technieken moet voldoen.	BIR 15.1.6

3. Richtlijn Cryptografische beheersmaatregelen

3.1. Algemene regels

UWV beveiligt de infrastructuur en systemen waar nodig door toepassing van cryptografische beheersmaatregelen. Op basis van een risicoafweging bepaalt de systeem-eigenaar in samenwerking met de Business Security Officer (BSO) of er aanvullend informatiebeveiligingsmaatregelen moeten worden genomen en welke maatregelen dat zijn. In het risicomanagement proces wordt het risico bepaald en in hoeverre de systeem-eigenaar daarin maatregelen moet, wil en kan treffen.

3.1.1. Classificatie

1. Het gebruik van cryptografische beheersmaatregelen om gegevens te beschermen wordt bepaald op basis van een classificatie van de vertrouwelijkheid van deze gegevens. Gegevens van UWV moeten in een vertrouwelijkheidsklasse worden ingedeeld op grond van de UWV Richtlijn Classificatie voor vertrouwelijkheid (CDO) en het BIV-beleid (BZ). Zie document "UWV BZ BIV Classificatie, paragraaf 3.4.2. - Zie SharePointpagina van Bestuurszaken (BZ).[4]

De toegekende vertrouwelijkheidsclassificatie is te vinden in het Canoniek Gegevensmodel UWV (CGM), te vinden op de DWU van de Data Office UWV, en in de Functionele Gegevensmodellen (FUGEMs) van de verschillende informatiesystemen.
Ook in de Risico Applicatie Lijst (RAL) wordt de vertrouwelijkheidsclassificatie bij het informatiesysteem vermeld. Deze RAL-lijst wordt beheerd bij BZ en wordt door de IB&P functionarissen binnen de UWV divisies onderhouden.

2. Cryptografische gegevens zoals certificaten en sleutels worden ingedeeld in de hoogste vertrouwelijkheidsklasse uit het UWV Classificatie model en zullen daarom ook beveiligd moeten worden met behulp van passende beveiligingsmaatregelen voor dit classificatie niveau.

3.1.2. Gebruik open standaarden internetveiligheid

UWV houdt zich aan de voor cryptografische beheersmaatregelen relevante open standaarden internetveiligheid die zijn voorgeschreven door Bureau Forum Standaardisatie[5]. Deze stelt open standaarden verplicht. Voor beveiliging van email- website- en appverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.
https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

Half jaarlijks worden er nieuwe streefbeeldafspraken gemaakt door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO): https://www.forumstandaardisatie.nl/thema/veilig-internet/streefbeeldafspraken

Voor alle organisaties binnen de publieke sector geldt een 'pas-toe-of-leg-uit' verplichting[6]. De verantwoordelijke eigenaar van de IT-middelen of ondersteunende processen ziet toe op naleving van de "pas toe of leg uit" van deze richtlijn.

3.1.2.1. Afwijken van de 'Pas toe of leg uit-lijst" (geen of andere cryptografische beheersmaatregelen)

Ten aanzien van de gestelde beveiligingseisen geldt het principe 'pas toe of leg uit'. Afwijkingen van deze richtlijn moeten worden gemotiveerd conform het "pas toe of leg uit" principe, waarbij de inherente risico's aantoonbaar worden afgewogen en de verantwoordelijk "eigenaar" of

[4] BIV-beleid: Ten tijde van deze Richtlijn Cryptografische Beheersmaatregelen was het UWV BIV-beleid in bewerking. De UWV Richtlijn classificatie zal opgenomen worden in het UWV BIV-beleid.
[5] https://www.forumstandaardisatie.nl/open-standaarden/over-open-standaarden/
[6] https://www.forumstandaardisatie.nl/nieuws/obdo-voert-op-advies-van-forum-wijzigingen-door-op-lijst-verplichte-standaarden

gedelegeerde tekent voor de restrisico's. Afwijken van het gebruik van de voorgeschreven overheidsvoorzieningen mag alleen als een dergelijke dienst of product in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert of om een andere reden die van bijzonder gewicht is. De afwijking en de reden daarvan moeten beschreven worden in de bedrijfsvoeringparagraaf van het jaarverslag. Dit is de betekenis van 'leg uit'.[7]

3.1.2.2. Lijst cryptografische beheersmaatregelen "pas toe of leg uit"

Zie ook de link naar: https://www.forumstandaardisatie.nl/open-standaarden/verplicht

	Lijst met relevante cryptografische beheersmaatregelen componenten:
Beschrijving	**Referentie**
Ades Baseline Profiles	https://www.forumstandaardisatie.nl/standaard/ades-baseline-profiles
AES	https://www.forumstandaardisatie.nl/standaard/aes
DKIM	https://www.forumstandaardisatie.nl/standaard/dkim
DMARC	https://www.forumstandaardisatie.nl/standaard/dmarc
DNSSEC	https://www.forumstandaardisatie.nl/standaard/dnssec
HTTPS en HSTS	https://www.forumstandaardisatie.nl/standaard/https-en-hsts-0
IP Sec	https://www.forumstandaardisatie.nl/standaard/ip-sec
NEN-ISO/IEC 27001	https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27001
NEN-ISO/IEC 27002	https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27002
SHA-2	https://www.forumstandaardisatie.nl/standaard/sha-2
SSH-2	https://www.forumstandaardisatie.nl/standaard/ssh-2
STARTTLS en DANE	https://www.forumstandaardisatie.nl/standaard/starttls-en-dane
TLS	https://www.forumstandaardisatie.nl/standaard/tls
WPA2 Enterprise	https://www.forumstandaardisatie.nl/standaard/wpa2-enterprise
X509	https://www.forumstandaardisatie.nl/standaard/x509
Digikoppeling	https://www.forumstandaardisatie.nl/standaard/digikoppeling
SAML	https://www.forumstandaardisatie.nl/standaard/saml
SPF	https://www.forumstandaardisatie.nl/standaard/spf
STIX en TAXII	https://www.forumstandaardisatie.nl/standaard/stix-en-taxii
IPv6	https://www.forumstandaardisatie.nl/open-standaarden/ipv6-en-ipv4

3.1.3. keymanagement beheer organisatie

Binnen UWV is het team Certificatenbeheer van ICT Infrastructuur Ontwikkeling en Regie verantwoordelijk voor de regie op het sleutel/certificaatbeheer. De ICT service providers zijn verantwoordelijk voor de uitvoering, voor zover in de contracten afgesproken.

1. Gebruik van eenzelfde certificaat in meerdere omgevingen is niet toegestaan!
   - Gebruik telkens andere certificaten in de Ontwikkelomgeving, Testomgeving, Acceptatieomgeving of in de Productie omgeving.

2. Gebruik van eenzelfde 'privé-sleutel' voor meerdere interne systemen is niet toegestaan!

3. Het gebruik van self-signed certificaten buiten de afdeling Certificatenbeheer om is niet toegestaan!

[7] https://www.forumstandaardisatie.nl/node/229

- De afdeling Certificatenbeheer van ICT-Services biedt zorgvuldig beheer op de individuele certificaten.
- Een self-signed certificaat is een zelf ondertekend certificaat dat niet uitgegeven of erkend is door een certificeringsorganisatie (een Certificate Authority). Het uitgifteproces van die certificaten is niet te controleren/auditeren, de certificaten hebben veelal geen einddatum en er vindt geen beheer plaats, bijvoorbeeld monitoring op kwetsbaarheden.
- Een belangrijk onderdeel van het gebruik van certificaten is het vertrouwen in een certificaat. Dit vertrouwen wordt belegd bij een CA. Bij een self-signed certificaat mist de vertrouwensrelatie en het beheer. Hierdoor kan een dergelijk certificaat per definitie niet vertrouwt worden.

4. Het bestaande proces voor beheer van certificaten is beschreven op PMWEB: https://samenwerken.sharepoint.uwv.nl/sites/DWU/ConcernICT/portaal%20PMWeb/Proceshuis/Online/BDC/index.html

De afdeling Certificatenbeheer heeft gedocumenteerde procedures voor sleutelbeheer waarin de volgende onderwerpen zijn beschreven:

a. Het verwerven/genereren van sleutel/certificaat materiaal;
b. De geldigheidsduur van de sleutels/certificaten;
c. De distributie van certificaten; Certificatenbeheer levert het certificaat aan de hosting leverancier in een wijzigingsverzoek.
d. Het hernieuwen van sleutels/certificaten;
e. Intrekken van cryptografische sleutels/certificaten;
f. Auditing en logging op sleutel/certificaat beheer in de vorm van het actief monitoren van de geldigheidsduur van certificaten en attendering van de productowners op het aflopen van de certificaten.
g. De opslag van certificaten; de hosting leverancier is verantwoordelijk voor opslag van de private-key.
h. Archiveren van cryptografische certificaten; de hosting leverancier is verantwoordelijk voor het archiveren van de private-key.
i. Vernietiging van certificaten; de hosting leverancier is verantwoordelijk voor het vernietigen van de private-key

3.1.4. Gebruik certificaten

Er moet te allen tijde zicht zijn op de inventaris van in gebruik zijnde certificaten. Het moet altijd inzichtelijk zijn hoe veel certificaten in gebruik zijn binnen de UWV infrastructuur, waar ze zijn geïmplementeerd en hoe ze gebruikt en gemanaged worden.

3.1.4.1. Gebruik PKI-O

UWV gebruikt Public Key Infrastructure overheid (PKI-O)-certificaten voor:

a. beveiliging van websites;
b. authenticeren op afstand van personen of services;
c. zetten van rechtsgeldige elektronische handtekeningen;
d. versleuteling van elektronische berichten (extern verkeer).

PKIoverheid-certificaten bieden aanvullende zekerheid voor de echtheid en de beveiliging van websites en waarborgen op basis van de Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites, mobiele apps of andere gegevensuitwisseling.

Voor het gebruik van certificaten binnen het UWV intranet is het advies om deze niet via een PKI-overheid of andere externe derde partij af te nemen. Daarmee geef je heel veel informatie weg over interne paden en systemen. Neem hiervoor contact op met ICT Infrastructuur Ontwikkeling en Regie, team Certificatenbeheer.

3.1.4.2. Interne certificaat server in eigen beheer van UWV.

Voor interne UWV netwerkverbindingen is het mogelijk[8] een interne voorziening (eigen CA) voor het uitgeven (self-signed) certificaten te gebruiken.
Dit dus in plaats van een externe geverifieerde vertrouwde Certificate Authority (CA).

Daarbij zijn de volgende voorwaarden van toepassing op de CA:

1. Er moet te allen tijde zicht zijn op de inventaris van uitgegeven self-signed certificaten. Het moet altijd inzichtelijk zijn hoe veel certificaten in gebruik zijn binnen de UWV infrastructuur, waar ze zijn geïmplementeerd en hoe ze gebruikt en gemanaged worden. De verantwoordelijkheid hiervoor ligt bij de systeem eigenaren.
2. Het is niet toegestaan om self-signed certificaten te gebruiken voor publieke netwerken in de A- en de P-omgevingen!
3. Self Signed Certificaten zijn uitsluitend bedoeld voor interne (intranet) verbindingen (o.a. A2A en A2C koppelingen);
4. Het beheer voor CA taken is centraal bij een aangewezen verantwoordelijke partij belegd. Contact loopt via ICT Infrastructuur Ontwikkeling en Regie, afdeling Certificatenbeheer.
5. De self-signed certificaten moeten continue worden gemonitord en worden beschermd (beveiligd).
6. Self-signed certificaten moeten periodiek (< 3 jaar) worden vervangen.
7. Administratief beheer wordt verzorgd door de UWV ICT infrastructuur Ontwikkeling en Regie (rekencentrum/datacentrum) leverancier(s);
8. De verantwoordelijkheid voor het administratief beheer ligt bij het UWV, bij de afdeling ICT services;
9. De verantwoordelijkheid voor het technisch beheer en onderhoud van de systemen ligt bij de hier bovengenoemde ICT infrastructuur leverancier;
10. Voor productkeuze geldt dat een door Nationaal Bureau voor Verbindingsbeveiliging (NBV) goedgekeurde of EU/NATO goedgekeurde product wordt gekozen.
    (Toelichting: Daar is naar dit soort zwakheden gekeken of het product voldoet aan SSD normen. Geeft geen volledige garantie, maar geeft wel weer een hogere drempel als risico beperkende maatregel.)

Een voorziening voor het automatiseren van het uitgeven en vervangen van self-signed certificaten kan in deze de handmatige CA beheer taken (deels) vervangen. Dat mitigeert de risico's voor het handmatig (her)uitgeven en onderhouden van deze self-signed certificaten. Het reduceert ook de kosten (personeel) op de beheerinspanning op de CA taken.

3.1.5. Organisatie certificatengebruik

In de divisie is de product owner verantwoordelijk voor het aanvragen, installeren en intrekken van certificaten. De BSO monitort certificatengebruik en is single-point-of-contact voor allertering bij aflopen van de certificaten.

A. Leg vast welke certificaten waar (in de organisatie en in systemen) in gebruik zijn.
B. Organiseer het certificatenbeheer met het team Certificatenbeheer van ICT Infrastructuur Ontwikkeling en Regie
C. Zij leggen vast welke partij de certificaten genereert.
D. Stel eisen aan het root-certificaat in lijn met deze Richtlijn Cryptografische beheersmaatregelen.

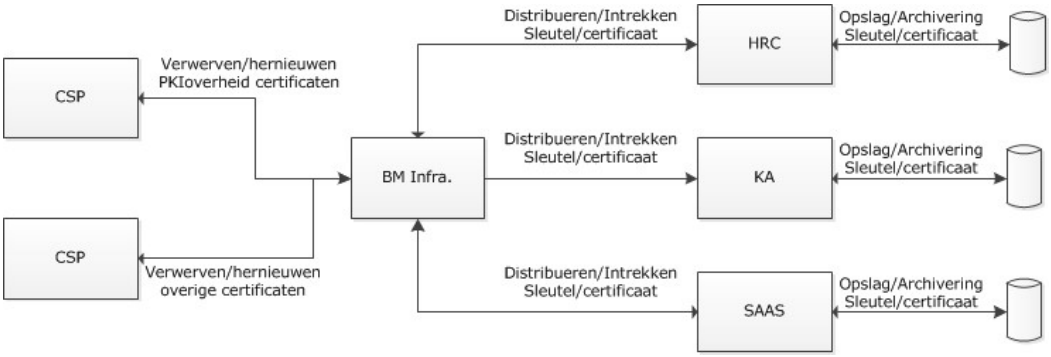
Leg bij alle nieuwe certificatenaanvragen de volgende informatie vast:

1. Product Owner die verantwoordelijk is voor het aanvragen en intrekken van het certificaat;

[8] Dit geldt voor leverancier DXC. Niet voor IBM.

2. Technisch Applicatie Beheerder die verantwoordelijke voor het installeren van het certificaat;
3. Wat is de verloopdatum van het certificaat?
   Het is nodig om dit te weten voor het tijdig verlengen van het certificaat.
4. Waarvoor wordt dit systeem of deze applicatie gebruikt?
5. Wat is de contactinformatie van de systeem- of applicatie eigenaar?
6. Betreft het een certificaat in bezit van een derde partij, maar wel cruciaal voor de bedrijfsvoering?
7. Welke CA heeft het certificaat uitgegeven, en wat is het CA pad dat wordt gebruikt (inclusief het certificaat van de root CA en alle tussenliggende CA's)?
8. Biedt het systeem of de applicatie de mogelijkheid de certificaten te vervangen?
9. Met welke techniek is het certificaat uitgegeven? Denk aan gebruikte algoritmen en sleutellengte.

Bron: Veilig beheer van digitale certificaten Factsheet FS-2012-02, versie 1.1, 14 december 2017.



Schematische weergave beheerproces[9]
Noot: Voor SAAS geldt altijd gebruik maken van PKI-O certificaten en niet het kunnen ontsluiten met gebruik van "overige" certificaten!

3.2. Specifieke regels

3.2.1. Gegevensuitwisseling via web portalen

In de onderstaande tabel wordt aangegeven welk doel wordt ondersteund door welke cryptografische techniek.

Doel	Cryptografisch middel
Identiteit vaststellen	Door inzet van cryptografie (**asymmetrische encryptie** obv public/private key) kan worden vastgesteld met wie er wordt gecommuniceerd tevens kan de ontvanger vaststellen dat de verzender ook daadwerkelijk de afzender is en niet iemand anders.
Vertrouwelijkheid waarborgen	Door inzet van cryptografie (**symmetrische encryptie**) kan ervoor worden gezorgd dat de inhoud van berichten en bestanden onleesbaar is voor derden (onbevoegden).

[9] CSP staat voor Certificaat Service Provider

Integriteit waarborgen	Door inzet van cryptografie (**hashing**) kan worden aangetoond dat gegevens tijdens transport of opslag (niet) zijn gewijzigd.
Authenticiteit vaststellen	Door inzet van cryptografische middelen kan de mate van betrouwbaarheid geborgd worden van de originaliteit en herkomst van de gegevens. Hiermee krijgt de ontvanger een zekere mate van garantie dat het bericht afkomstig is van de identiteit, die als ondertekenaar bij het bericht staat vermeld. (**signing**)
Onweerlegbaarheid waarborgen	Door inzet van cryptografische middelen kan worden aangetoond dat bepaalde gebeurtenissen of handelingen hebben plaatsgevonden, zoals het verzenden en ontvangen van elektronische documenten.

1. Cryptografische beheersmaatregelen moet er voor zorgen dat de gegevensuitwisseling tussen UWV en klant voldoet aan de volgende criteria voor informatiebeveiliging[10]:
   a. de integriteit van de gegevens moet gewaarborgd zijn;
   b. de vertrouwelijkheid van de gegevens moet gegarandeerd zijn;
   c. beide partijen moeten zekerheid hebben over de onweerlegbaarheid (controleerbaarheid) van een transactie.
   d. authenticiteit, je wilt zeker weten dat je informatie ontvangt van degene waar je iets van verwacht.

2. Om integriteit en vertrouwelijkheid van de inhoud van gegevensuitwisseling alsmede de onweerlegbaarheid van een transactie te garanderen, volgt UWV de NCSC TLS richtlijnen.

3. UWV moet gebruik maken van TLS configuraties die forward secrecy[11] bieden en die als goed of voldoende zijn beoordeeld door het NCSC[12].

4. Op basis van een risicoanalyse waarin rekening wordt gehouden met de classificatie voor de transport versleuteld in overeenstemming met deze richtlijn.

3.2.2. Beheer toegang tot web portalen

De EU richtlijn EIDAS[13] over toegankelijkheid van overheidswebsites en apps heeft als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor Nederlandse burgers en bedrijven bij de (semi-)overheid. Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit.

1. Voor burgers is DigiD het middel binnen het e-ID stelsel waarmee zij toegang kunnen krijgen tot UWV web applicaties.

2. Werkgevers en zakelijke klanten moeten in het e-ID stelsel gebruik gaan maken van eHerkenning om toegang te krijgen tot UWV applicaties. Dat kan worden gezien als een soort DigiD voor bedrijven. Een belangrijk verschil is dat DigiD wordt verstrekt door de overheid en eHerkenning door commerciële bedrijven.

3. UWV schrijft op basis van de classificatie van de uit te wisselen gegevens het noodzakelijke betrouwbaarheidsniveau van eHerkenning voor.

[10] Beschikbaarheid, dit criterium voor informatiebeveiliging is in dit verband niet relevant voor encryptie.
[11] Forward secrecy is een techniek om de vertrouwelijkheid van TLS-communicatie te blijven waarborgen als de geheime sleutel van een certificaat naderhand gestolen wordt.
[12] Zie de NCSC ICT-beveiligingsrichtlijnen voor TLS: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html
[13] https://www.digitaleoverheid.nl/dossiers/eidas/

4. Voor gevallen waar geen eHerkenning beschikbaar is, is maatwerk noodzakelijk. Bijvoorbeeld de toegang van gemeenteambtenaren tot UWV gegevens voor de uitvoering van de WMO. Voor maatwerk gelden dezelfde eisen ten aanzien van beveiliging als voor DigiD en eHerkenning.

3.2.3. Gegevensuitwisseling tussen interne UWV- en externe applicaties

Het betreft hier het gegevensverkeer tussen interne UWV applicaties die gekoppeld zijn aan applicaties buiten het UWV domein. Bijvoorbeeld de doorgifte van belastinggegevens van UWV klanten en UWV personeel aan de Belastingdienst of de gegevens van uitkerings- en salarisbetalingen aan banken.

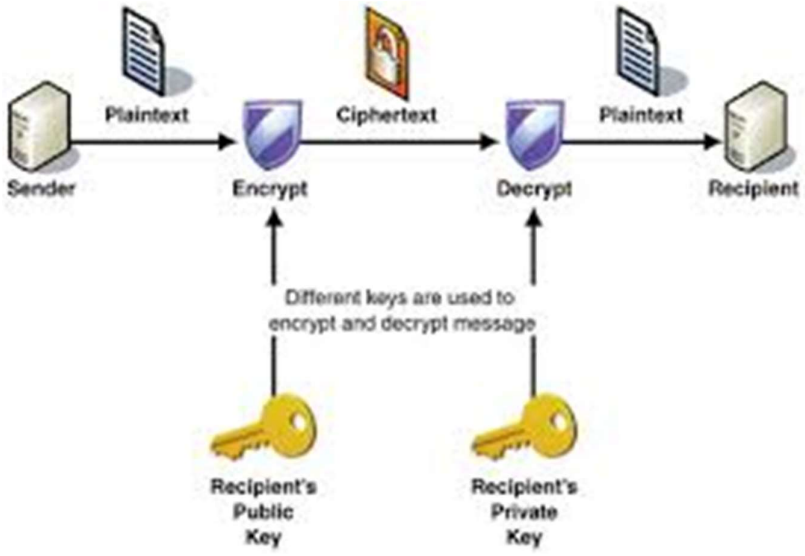
Kenmerkend voor applicatie-applicatieverkeer is:

I. Er is geen menselijke tussenkomst;
II. Het gaat om communicerende applicaties (A2A), de natuurlijke persoon is t.a.v. deze communicatie voor gegevensuitwisseling, buiten beeld;
III. Het kan dan zowel om berichtuitwisseling als bulk uitwisseling gaan.

Vergelijkbaar met gegevensuitwisseling via web portalen moeten bij applicatie-applicatieverkeer het 'kanaal' en de 'inhoud' op twee verschillenden manieren worden beveiligd.

De wijze van beveiliging is natuurlijk altijd afhankelijk van de UWV vertrouwelijkheidsclassificatie van de gegevens. Zie document "UWV BZ BIV Classificatie, paragraaf 3.4.2. - Zie SharePointpagina van Bestuurszaken (BZ).[14]

De identificatie en authenticatie gebeurt met certificaten voor SSL/TLS. Dat is het assymetrische encryptie deel bij opzetten van het secure channel. Van belang hierbij is dat er keuze is tussen 1 zijdige en 2-zijdige authenticatie.

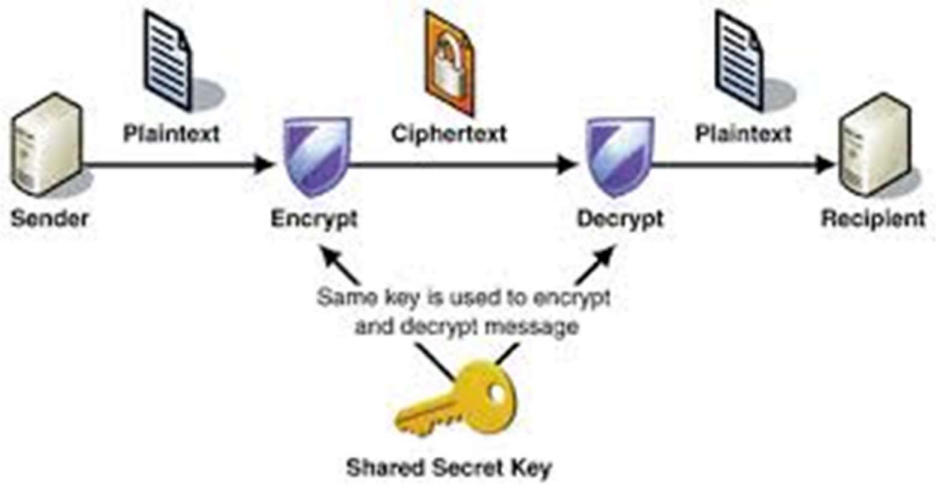


Afbeelding 1: Asymmetrische encryptie

Het afschermen van (vertrouwelijke) informatie kan door encryptie tijdens gebruik, opslag of transport van het bericht of bestand, door symmetrische encryptie. Bij voorkeur vindt de symmetrische encryptie transparant voor de eindgebruiker plaats. Omdat symmetrische encryptie zich vaak afspeelt op het niveau van verbindingen, netwerken en systemen is dat ook meestal het geval. Bekende voorbeelden hiervan zijn de VPN's (Virtual Private Network), TLS (Secure Socket

[14] BIV-beleid: Ten tijde van deze Richtlijn Cryptografische Beheersmaatregelen was het UWV BIV-beleid in bewerking. De UWV Richtlijn classificatie zal opgenomen worden in het UWV BIV-beleid.

Layer) en Wi-Fi encryptie (WPA). Daar waar de encryptie zich op applicatieniveau afspeelt, is vaak nog interactie van de eindgebruiker vereist. Voorbeelden hiervan zijn e-mail encryptie en aparte software voor encryptie van bestanden om deze op draagbare media op te slaan of als bijlage met e-mail te versturen. De encryptie is uiteindelijk zo sterk als de mate waarin de cryptografische sleutel geheim gehouden kan worden voor onbevoegden.



Afbeelding 2: Symmetrische encryptie

Normen:

1. UWV moet voor applicatie-applicatie uitwisseling gebruik maken van digitaal certificaten waarin beide bovenstaande vormen (transport TLS / inhoud cryptografische beheersmaatregelen) van beveiliging worden gecombineerd, dus 2-zijdige authenticatie én beveiligd transport.

2. Op basis van de classificatie voor vertrouwelijkheid van de gegevens, worden deze gegevens tijdens transport versleuteld of gehashed in overeenstemming met deze richtlijn. Afhankelijk van de doelen van de cryptografische beheersmaatregelen wilt bereiken kun je om de vertrouwelijkheid te borgen versleuteling toepassen; om de integriteit te waarborgen is hashen nodig.

3. Voor gegevensuitwisseling met externe partijen is signing van berichten een vereiste. Afhankelijk van de vertrouwelijkheidsklasse van de gegevens kunnen aanvullende beheersmaatregelen toegepast worden.

4. Voor de interne en externe uitwisseling is identificatie/authenticatie/autorisatie een vereiste. Afhankelijk van de vertrouwelijkheidsklasse van de gegevens kan 2factor- of meerfactor authenticatie een vereiste zijn.

5. Voordat er sprake kan zijn van gegevensuitwisseling met een extern betrokken partij moet er een uitwisselingsovereenkomst met UWV zijn afgesloten[15]. De beveiligings- en/of bewerkersovereenkomst is onderdeel van de contracten set met de leverancier.
Bij UWV kennen we hiervoor de Beveiligings- en bewerkersovereenkomst (BVO). Deze bevat de afspraken op het gebied van beveiliging. Denk hierbij aan het de beveiligingsorganisatie van de leverancier, de bescherming van onze gegevens en het toepassen van SSD.

3.2.4. Gegevens in opslag

1. Op basis van een risicoanalyse waarin rekening wordt gehouden met de UWV classificatie voor de vertrouwelijkheid van de gegevens kan versleuteling in opslag in overeenstemming met deze richtlijn en de UWV richtlijn fysieke gegevensdragers noodzakelijk zijn.

[15] Zie BIR 10.8.2 Uitwisselingsovereenkomsten.

Dit is in de context natuurlijk altijd afhankelijk van de UWV vertrouwelijkheid classificatie van de gegevens in opslag! Geldt ook voor analyseomgevingen. Op applicatie-nivo kan dit opname in de applicatie-architectuur en inrichting van Encryptie-services vergen.

2. Vertrouwelijkheidsklasse 3 gegevens moeten in databases en anders opgeslagen gegevens in bestanden binnen UVW datacenters zijn afgeschermd. Hiervoor is een risicoanalyse en een GEB noodzakelijk. Wanneer voor deze gegevens op basis van een risicoanalyse is vastgesteld dat de beveiligingsmaatregelen die reeds zijn getroffen om de vertrouwelijkheid te waarborgen nog een restrisico met zich meebrengen, zijn cryptografische beheersmaatregelen noodzakelijk. (medisch beroepsgeheim, zie document "UWV BZ BIV Classificatie BIV, paragraaf 3.4.2. - *Zie SharePointpagina: Overzicht IB&P beleid en richtlijnen)*[16]

3. Op basis van de gegevensclassificatie moeten draagbare computers, tablets, smartphones, etc. de mogelijkheid hebben om de toegang te beschermen. Dit kan o.a. via authenticatie door middel van bijvoorbeeld een wachtwoord, pincode, biometrische herkenning en versleuteling van de gegevens. Deze versleuteling moet voldoen aan de huidige stand der techniek voor bulkversleuteling.
(Denk hier aan bijvoorbeeld: een schijfencryptie-programma (bijvoorbeeld "BitLocker of VeraCrypt") ontworpen om gegevens te beschermen door cryptografische beheersmaatregelen (gegevensstationsversleuteling) voor alle gegevens en opgenomen in de Microsoft-besturingssystemen Windows Vista, Windows Server 2008, Windows 7, Windows 8 en Windows 10.)

4. Voor fysieke gegevensdragers zonder operating systeem zoals bijvoorbeeld usb-sticks geldt de UWV richtlijn voor fysieke gegevensdragers "IB&P Richtlijn Beveiliging fysieke gegevensdragers en transport Versie 4".
(Zie SharePointpagina: Overzicht IBenP beleid en richtlijnen)

3.2.5. Gebruik gegevens intern UWV

De context is natuurlijk bepalend voor de UWV vertrouwelijkheidsclassificatie van de gegevens!

1. Toegang tot UWV IT-middelen wordt beheerst met een beveiligde inlogprocedure die aansluit bij het belang van het bedrijfsproces.

2. De inloggegevens worden tegen afluisteren beschermd door gebruik van geschikte cryptografische beheersmaatregelen, gegeven de stand der techniek.

3. Toegang tot besturingssystemen, kritische toepassingen of toepassingen met een hoog belang om deze te willen of moeten afschermen, wordt verleend op basis van multi factor authenticatie.

4. Gegevensuitwisseling intern UWV (o.a. tussen UWV applicaties onderling, interne koppelingen via middleware zoals bijvoorbeeld via een servicebus of een API Gateway) wordt beschermd tegen afluisteren en aanpassen door het toepassen van geschikte cryptografische beheersmaatregelen, gegeven de stand der techniek. Intern UWV, bij web services moet gebruik worden gemaakt van HTTPS of SFTP (voorkeur)/FTPS (uitzondering) (zie ook SSD 4).

5. Bij gegevensuitwisseling (tussen UWV divisies) moet ook een vorm van uitwisselingsoverkomsten afgesloten worden. Een operationeel servicecontract (voorwaardelijke levering condities) dat leidend is voor het technische service contract is een algemene markt standaard. Gemaakte afspraken kunnen dan op basis van de voorwaardelijke condities worden gelogd waar nodig en worden gemonitord (controleerbaarheid/audit trial). SI heeft een SERVICE BIBLIOTHEEK (REGISTER) recent in gebruik genomen. Deze is voor intern gebruik UWV brede inzet bedoeld om de operationele service contracten centraal te registeren.

[16] BIV-beleid: Ten tijde van deze Richtlijn Cryptografische Beheersmaatregelen was het UWV BIV-beleid in bewerking. De UWV Richtlijn classificatie zal opgenomen worden in het UWV BIV-beleid.

3.3. Beveiligen van email

UWV verwerkt vertrouwelijke informatie en wisselt het uit met steeds meer partijen. Door toenemende bedreigingen vanuit internet, vormt e-mail steeds meer een risico voor de veiligheid en vertrouwelijkheid van privacygevoelige informatie.
Gegevens worden tegen afluisteren beschermd door toepassing van geschikte cryptografische beheersmaatregelen, gegeven de stand der techniek. Voor de intranet mail voorziening op basis van een business behoefte wordt dit via de email servers van KPN verzorgd. Privacygevoelige gegevens mogen niet uitgewisseld worden via de e-mail. Daar zijn specifieke berichtenservices voor, afhankelijk van de partij waarmee de gegevens uitgewisseld worden (klant, werkgever, arts, partnerorganisatie, etc.)

Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.