

Digital Architecture Design Day

NORA Familie: Bouw mee aan een veilige overheidsdienstverlening

5 oktober 2023

Marieke Vos, Guus van den Berg en Joris Dirks

Wat is de NORA Familie?

1. Kennis-community van architecten & architecturen in de publieke sector, met de wiki noraonline.nl als publiek kennisplatform
2. Inhoudelijk eigenaar van de NORA Kernwaarden van Dienstverlening, Kwaliteitsdoelen, Architectuurprincipes & Implicaties



Centrum Informatiebeveiliging en Privacybescherming (CIP)

- Publiek-private netwerkorganisatie, opgericht in 2012
 - N.a.v. hack DigiNotar -> via Manifestgroep
 - Vier Founding Fathers: SVB, DUO, Belastingdienst en hoofdsponsor UWV
- Opdrachten vanuit Ministeries BZK (Baseline Informatiebeveiliging Overheid), EZK (Inkoopeisen Cybersecurity Overheid) en CIO-Rijk/PAR
- Het CIP kernteam bestaat uit 20 medewerkers en bedient een netwerk van zo'n 4500 IB&P professionals
- Het CIP motto: Voor allen, door allen!

Thema Beveiliging

Beveiliging - NORA Online

https://www.noraonline.nl/wiki/Beveiliging#

Account aanmaken Inloggen

Pagina **Overleg** Lezen Brontekst bekijken Geschiedenis weergeven Tools Meer Doorzoek NORA Online

NORA
Nederlandse Overheid
Referentie Architectuur

NORA
Nieuws & Agenda
Laatste wijzigingen
Blijf op de hoogte
Hulp & contact

Ecosysteem
NORA Familie
GDI Architectuur

Architectuurspraken
Overzicht
Kernwaarden
Kwaliteitsdoelen
Architectuurprincipes
Implicaties
Wijzigingen 1-1-2023

Lijsten & Verwijzingen
Beleidskaders
Standaarden
Bouwstenen
Begrippen
Architecturen
Gegevens-
woordenboeken

Thema's
Overzicht
Beveiliging
Basisconcept van
Dienstverlening
AI & Algoritmen

Beveiliging

NORA > Thema's > Beveiliging > Beveiliging

Agenda

- donderdag 21 september 2023 - [Expertgroep Beveiliging september 2023](#)
- donderdag 2 november 2023 - [Expertgroep Beveiliging november 2023](#)
- donderdag 14 december 2023 - [Expertgroep Beveiliging december 2023](#)

→ [Volledige agenda NORA](#)

9 februari 2023 - [Help ons om de BIO Thema-uitwerkingen voor jou werkbaar te maken ...](#)

27 september 2022 - [Ingrijpende wijzigingen aan de NORA Bindende Architectuurspraken per 1-1-2023...](#)

5 april 2022 - [Kick-off NORA Expertgroep Beveiliging op 11 april 2022 _doe jij mee? ...](#)

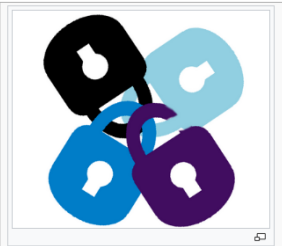
📧: → [AI het NORA Nieuws](#)

Inhoud [verbergen]

- 1 [Wat is beveiliging?](#)
- 2 [Organisatiebeleid](#)
- 3 [In project of systeem](#)
- 4 [Normen & eisen](#)
- 5 [Semantische data voor dit onderwerp](#)
 - 5.1 [Relaties](#)
 - 5.2 [Wordt toegepast in](#)
 - 5.3 [Past toe](#)
 - 5.4 [Visualisatie \(werkt nog niet goed\)](#)

Wat is beveiliging? [bewerken]

Beveiliging, of te wel integrale beveiliging, is het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen voor de beveiliging van de Te Beschermen Belangen op basis van risicomanagement¹. Te Beschermen Belangen zijn personen, informatie, informatiesystemen, materieel, goederen, imago en objecten, waarbij in geval van compromittering, of de mogelijkheid van compromittering, nadelige gevolgen, of een risico daarop, kan ontstaan voor de vertrouwelijkheid, beschikbaarheid en integriteit van de primaire processen van de rijksoverheid, delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries¹.



Beveiliging

Onderdeel van [Thema's](#)

Contact

Guus van den Berg
Guus.vandenberg@cip-overheid.nl

Status

Dit thema wordt momenteel opnieuw bekeken door de [Expertgroep Beveiliging](#)

Inhoud Beveiliging

[Beveiliging/metamodel](#)

[Beveiliging/index](#)

Organisatiebeleid

Doel: Toepasbare informatie

Wie heeft wat wanneer nodig?

- Enterprise, business, informatie, solution architect
- Op verschillende momenten in life cycle systeem, dienst, proces
- In alle bestuurslagen en types (overheids-)organisaties
- In verschillende ketens, domeinen, sectoren

Scope: dat wat generiek is, plus verwijzingen naar wat specifiek is

Vraag aan jullie:

Wat hebben architecten in de publieke sector nodig om hun werk goed te doen, als het gaat om informatieveiligheid?

Of

Wat heb jij nodig om je werk goed te kunnen doen, als het gaat om informatieveiligheid?

Uitleg werkvorm

Doe wat je zegt...



Wat is er al bij anderen?
Wat hebben we zelf al?

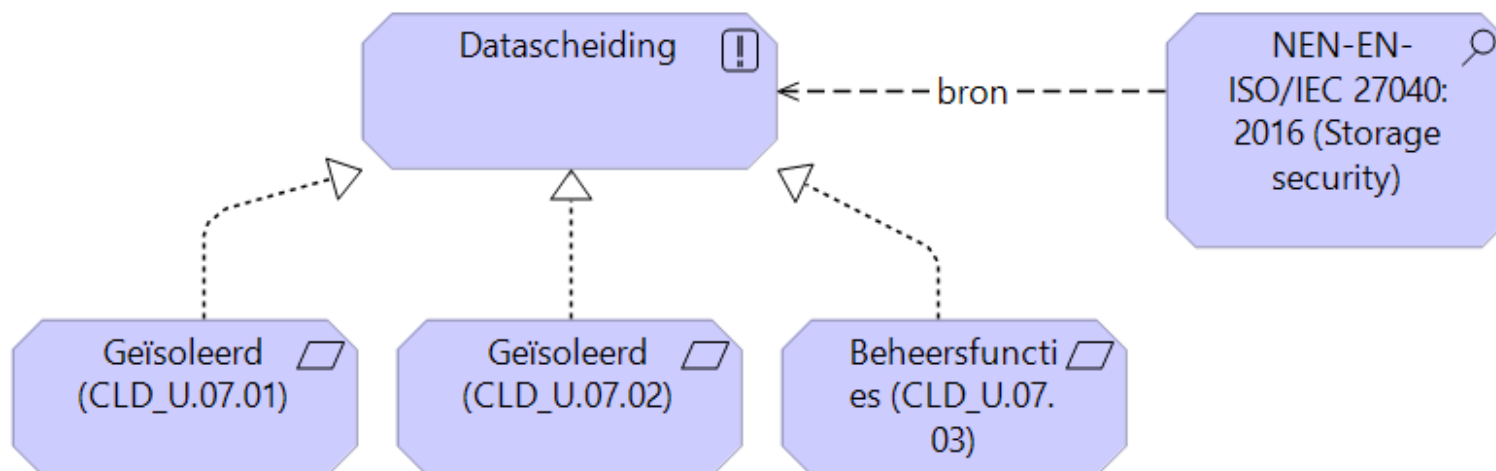
En is dat bruikbaar?

Content

- Sinds 2018: Actuele BIO thema-uitwerkingen (normenkaders)
- Sinds 2018: Privacy-baseline
- Sinds 2013:
 - Kaders
 - Beheersrichtlijnen
 - Beveiligingspatronen

Thema-uitwerkingen van de BIO

- Thema-uitwerkingen ('Normenkaders'):
 - Gedetailleerder: *hoe*.
 - Verwijst naar BIO, ISO en domein-standaarden
 - Applicatieontwikkeling, cloud, toegangsbeveiliging...



DADD NORA Familie Beveiliging

Datascheiding

NORA > Thema's > ISOR (Information Security Object Repository) > Scheiding van data
 ISOR: Scheiding van data

Versie 2.0 van 1 juni 2021 van de BIO Thema-uitwerking Clouddiensten is vervangen door versie 2.1 van 29 oktober 2021. De wijzigingen betreffen met name de uniformering van objectdefinities en objectnamen in en tussen [BIO Thema-uitwerkingen](#).
 Versie 2.1 in PDF-formaat is op de website [CIP-overheid/producten](#) gepubliceerd.

[Exporteer naar RDF](#)

Objectdefinitie

Betreft het duurzaam isoleren van Cloud Service Consumer (CSC)-data van andere CSC's.

Objecttoelichting

Het isoleren van de data (in bewerking of in rust) van de CSC, van alle data van de Cloud Service Provider (CSP) en van de data van andere CSC's. Duurzame scheiding van CSC-data en van de data van andere bedrijven (secure multi-tenancy), zowel tijdens transport, in bewerking als opslag, is randvoorwaardelijk voor het afnemen van veilige clouddiensten.

Criterium

CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam **geïsoleerd** te zijn van **beheerfuncties** en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.

Doelstelling

Zorgen dat de data van of in beheer van de CSC alleen toegankelijk is voor deze CSC.

Risico

Andere CSC's en de CSP krijgen toegang tot de data of in beheer van de CSP en vice versa.

Indeling binnen ISOR

Dit beveiligingsprincipe:

- is gericht op het [Beveiligingsaspect Uitvoering](#);
- valt binnen de [Invalshoek Functie](#).

(Klik om uitleg open/dicht te klappen)

Grondslag

De grondslag voor dit principe is [NEN-EN-ISO/IEC 27040:2016 \(Storage security\) 7.7.4](#)



Onderliggende normen

| ID | Conformiteitsindicator | Stelling |
|-----------------------------|------------------------|---|
| CLD_U.07.01 | Geïsoleerd | Permanente isolatie van gegevens wordt gerealiseerd binnen een multi-tenantarchitectuur. Patches en aanpassingen van applicaties en infrastructuur worden op een gecontroleerde wijze gerealiseerd voor alle clouddiensten die de Cloud Service Consumer (CSC) afneemt. |
| CLD_U.07.02 | Geïsoleerd | Isolatie van Cloud Service Consumer (CSC)-gegevens wordt gegarandeerd door deze onder alle bedrijfsomstandigheden minimaal logisch te scheiden van de data van andere CSC's. |
| CLD_U.07.03 | Beheerfuncties | De bevoegdheden voor het inzien of wijzigen van Cloud Service Consumer (CSC)-data en/of van encryptiesleutels door beheerfuncties en beheerders worden gecontroleerd verleend en het gebruik van deze rechten wordt gelogd. |



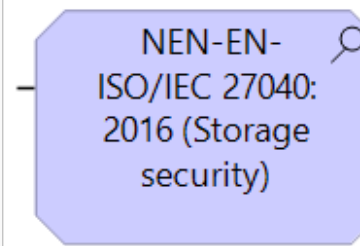
ID: CLD_U.07
Beveiligingsprincipe
 Versie: 2.1
 Status: Actueel
 Publicatiedatum: 29-10-2021
 Redactionele wijzigingsdatum: 17-1-2022

Indeling

[Beveiligingsaspect:](#)  [Uitvoering](#)
[Invalshoek:](#)  [Functie](#)

Verwante principes

- [BIO Thema-uitwerking Clouddiensten](#)
- [Binnen dit normenkader en beveiligingsaspect](#)
- [Alle Normenkaders](#)
- [Alle Beveiligingsprincipes](#)
- [Alle Normen](#)
- [Beveiligingsaspecten](#)
- [ISOR](#)



- Thema
- Ge
- Ver
- App

Thema Beveiliging

- Beleid voor overheden (kaders & architectuuraanpak)
- Beheer: bedrijfsfuncties, control
- Principes en beheersrichtlijnen
- Beveiligingspatronen & beschouwingsmodellen

Beheersmaatregelen (2013)

Beheersmaatregelen binnen het thema Beveiliging/Transactie:

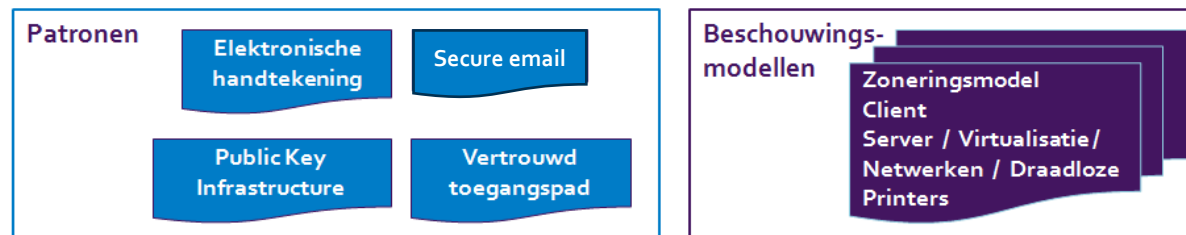
- [Integriteitscontrole van het bericht](#)
De integriteit (authenticiteit) van het verzonden bericht wordt vastgesteld met behulp van een elektronische handtekening.
- [Wederzijdse authenticatie](#)
Alvorens een transactie mogelijk is, wordt de identiteit van de ontvanger of ontvangend systeem, en de identiteit van de zender van het bericht vastgesteld door middel van authenticatie.

Relevante [beveiligingspatronen](#) voor het thema Beveiliging/Transactie:

- [Patroon voor elektronische handtekening](#)
- [Patroon voor public key infrastructure](#)
- [Patroon voor secure email](#)
- [Patroon voor vertrouwd toegangspad](#)

Beheers-
maatregelen

Implementatie-
richtlijnen



Beheer Wederzijdse authenticatie

[NORA](#) > [Thema's](#) > [Beveiliging](#) > Wederzijdse authenticatie

Eis: Alvorens een transactie mogelijk is, wordt de identiteit van de ontvanger of ontvangend systeem, en de identiteit van de zender van het bericht vastgesteld door middel van authenticatie.

Realiseert [\[bewerken\]](#)

Wederzijdse authenticatie realiseert het/de afgeleide principe(s):

- [Onweerlegbaarheid \(principe\)](#)

Implicaties [\[bewerken\]](#)

De volgende implementatierichtlijnen zijn een uitwerking van *Wederzijdse authenticatie*:

1. Er is een betrouwbare berichtendienst in het besloten netwerkverkeer. Hierbij worden verzending en ontvangst van berichten bevestigd door de berichtendienst of worden hiervoor in de applicaties extra functies opgenomen.
2. Bij een onvertrouwd netwerk:
 - Een PKI voldoet aan de daarvoor geldende standaarden; bij de overheid die van de [PKIoverheid](#);
 - De elementen die het bewijs vormen van een elektronische handtekening worden in de vorm van een juridisch logbestand zodanig samen met de originele data bewaard dat datzelfde bewijs in de normale werkstroom van het bedrijfsproces altijd weer is te reproduceren;
 - De ontvangen berichten worden onmiddellijk na ontvangst in de juridische logging vastgelegd voordat enige bewerking met toepassingssoftware aan de orde is;
 - De verzonden berichten worden in de laatste fase van verwerking onmiddellijk voordat verzending plaatsvindt in de juridische logging vastgelegd (BIR (Baseline Informatiebeveiliging Rijksdienst))

[Beheersmaatregelen](#) binnen het thema Beveiliging/Transactie:

- [Integriteitscontrole van het bericht](#)
De integriteit (authenticiteit) van het verzonden bericht wordt vastgesteld met behulp van een elektronische handtekening.
- [Wederzijdse authenticatie](#)
Alvorens een transactie mogelijk is, wordt de identiteit van de ontvanger of ontvangend systeem, en de identiteit van de zender van het bericht vastgesteld door middel van authenticatie.

Relevante [beveiligingspatronen](#) voor het thema Beveiliging/Transactie:

- [Patroon voor elektronische handtekening](#)
- [Patroon voor public key infrastructure](#)
- [Patroon voor secure email](#)
- [Patroon voor vertrouwd toegangspad](#)

Beheers-
maatregelen

Implementatie-
richtlijnen

Patronen

Ele
ha

Pub
Infrast

Wederzijdse
authenticatie

Wederzijdse authenticatie is een eis
([Beheersmaatregel](#))

Status: Concept

Realiseert Afgeleid Principe:

[Onweerlegbaarheid \(principe\)](#)

Thema: [Beveiliging/Transactie](#)

Bron: [BIR \(Baseline Informatiebeveiliging Rijksdienst\)](#),

BIR/ISO 27001:2005 10.8.4, 10.9.2,
12.2.3, ISO 27001:2013 14.1.3

Patronen (2013)

Beheersmaatregelen binnen het thema Beveiliging/Transactie:

- [Integriteitscontrole van het bericht](#)
De integriteit (authenticiteit) van het verzonden bericht wordt vastgesteld met behulp van een elektronische handtekening.
- [Wederzijdse authenticatie](#)
Alvorens een transactie mogelijk is, wordt de identiteit van de ontvanger of ontvangend systeem, en de identiteit van de zender van het bericht vastgesteld door middel van authenticatie.

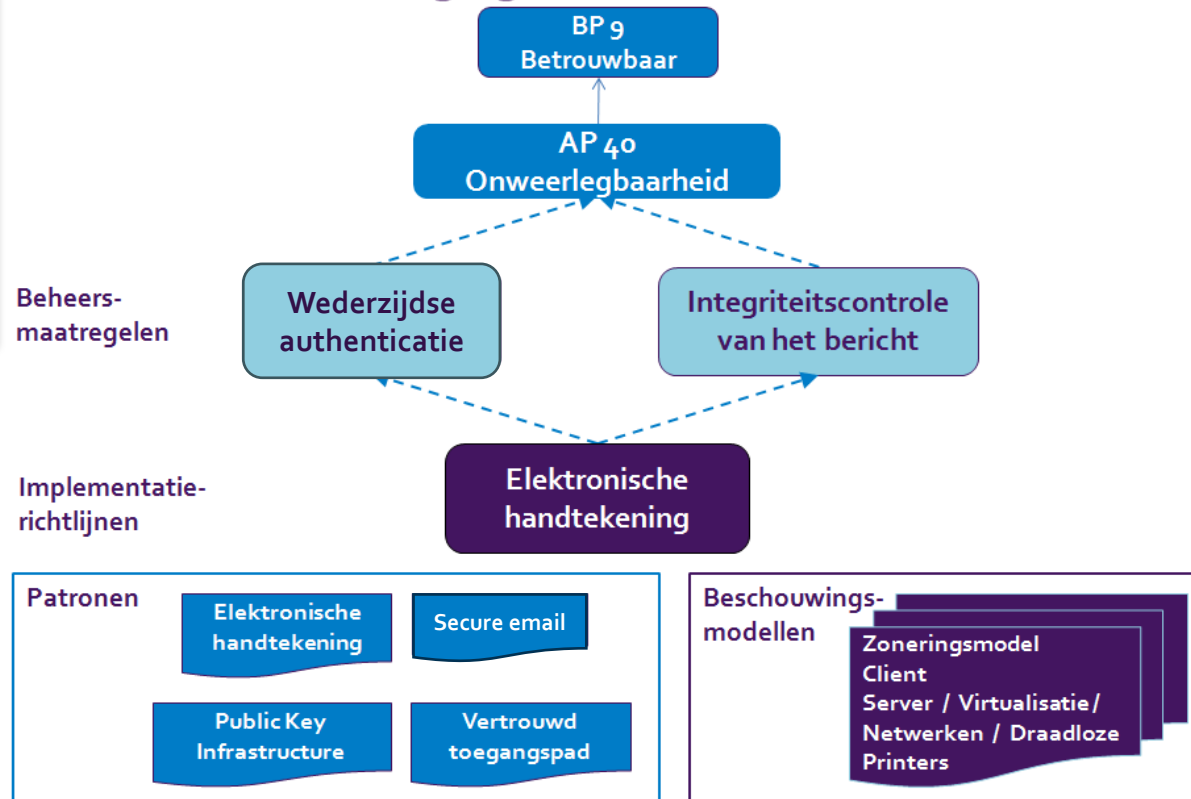
Relevante beveiligingspatronen voor het thema Beveiliging/Transactie:

- [Patroon voor elektronische handtekening](#)
- [Patroon voor public key infrastructure](#)
- [Patroon voor secure email](#)
- [Patroon voor vertrouwd toegangspad](#)

Beheers-
maatregelen

Implementatie-
richtlijnen

Beveiligingsthema Transactie



Patr

Beveiliging

Wederzijdse authenticatie

Beheersmaatregelen

Implementatierichtlijnen

Patronen

Elektronische handtekening

Public Key Infrastructure

Beheersmaatregelen binnen het thema Beveiliging/Transactie:

- [Integriteitscontrole van het bericht](#)
De integriteit (authenticiteit) van het verzonden bericht wordt vastgesteld met behulp van een elektronische handtekening.
- [Wederzijdse authenticatie](#)
Alvorens een transactie mogelijk is, wordt de identiteit van de ontvanger of ontvangend systeem, en de identiteit van de zender van het bericht vastgesteld door middel van authenticatie.

Relevante beveiligingspatronen voor het thema Beveiliging/Transactie:

- [Patroon voor elektronische handtekening](#)
- [Patroon voor public key infrastructure](#)
- [Patroon voor secure email](#)
- [Patroon voor vertrouwd toegangspad](#)

Patroon voor secure email

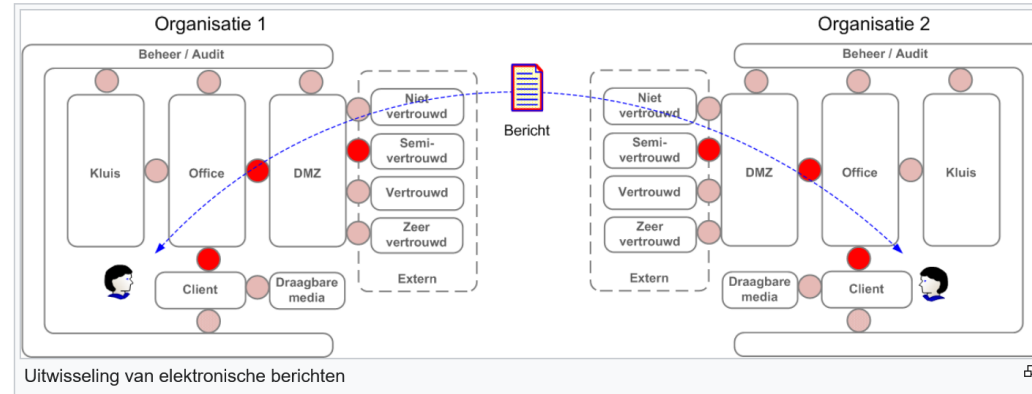
[NORA](#) > [Thema's](#) > [Beveiliging](#) > [Beveiligingspatronen](#) > [Transactie](#) > Patroon voor secure email

Criteria [\[bewerken\]](#)

Vertrouwelijkheid, Integriteit

Context [\[bewerken\]](#)

Men wisselt e-mailberichten uit tussen verschillende organisaties of natuurlijke personen. Daarbij kan niet worden uitgegaan van een vertrouwd (toegangs)pad. Toch vraagt de inhoud van het bericht om een bepaald niveau van vertrouwelijkheid. Ook wil de zender dikwijls meer zekerheid hebben over het tijdig en goed afleveren van het bericht aan de juiste ontvanger.



Probleem [\[bewerken\]](#)

Tijdens transport van de e-mail tussen de verzender en de ontvanger vormen ongewenst inzien en aanpassingen van het e-mailbericht door een buitenstaander risico's. De betrokkenen (zowel zender als ontvanger(s)) hebben geen enkele garantie dat een e-mailbericht onderweg niet wordt ingezien door andere partijen (vertrouwelijkheid). Ook is er geen garantie dat het bericht door een buitenstaander niet gewijzigd is (integriteit). Een derde probleem is dat de afzender niet eenduidig kan bewijzen dat het bericht verzonden is en dat het bericht de geadresseerde heeft bereikt. De onweerlegbaarheid van de verzending en van de aankomst op de bestemde tijdstippen daarvan is normaliter niet geregeld.

Oplossing [\[bewerken\]](#)

De oplossing is het beveiligen van het bericht voordat het de verzender bereikt. Het bericht wordt dan met een elektronische handtekening afgeleverd.

Wat kunnen we hergebruiken / doorontwikkelen?

Kijk in een groepje naar de vellen met 'nodig':

- Wat is er al op dit gebied? (producten, gremia, kenniscentra, resources)
- Is die direct (her-)bruikbaar?
 - Zo nee waarom niet?
 - Zo ja voor wie / in welke context?
- Is er een goed startpunt voor doorontwikkeling?
- Weet je mensen of partijen om hier bij te betrekken?



Meer informatie



[Beveiliging - NORA Online](#)

[Privacy - NORA Online](#)

CIP-community

The screenshot shows the CIP website's news section. The navigation bar includes 'Nieuws', 'Fora', 'Groepen', and 'Over CIP'. Under 'Recent nieuws', there are two article thumbnails. The first has the text 'Lang niet alle deuren goed op slot' over an image of a door handle. The second has the hashtag '#zoBouw' over an image of people in a meeting. A large QR code is overlaid on the right side of the news section.

CIP-YouTube kanaal



CIP-website

The screenshot shows the CIP website homepage. The header includes the CIP logo and navigation links: 'Home', 'Voor wie', 'Producten', 'Workshops', 'Over CIP', 'Contact', and 'Actueel'. The main content area features the text 'Samenwerken aan informatieveiligheid en privacybescherming' with two buttons: 'Over CIP' and 'Contact'. Below this, there is a section titled 'Voor wie' with a small image of a hand holding a document labeled 'Grip op'. A large QR code is overlaid on the bottom right of the homepage screenshot.

CIP-LinkedIn



Schuif eens aan bij de NORA Familie

meedenken - kennis opdoen - oplossingen delen

Informatie:

noraonline.nl

[lijst architecturen \(noraonline\)](#)

[Sessies op DADD](#)

Contact:

nora@ictu.nl

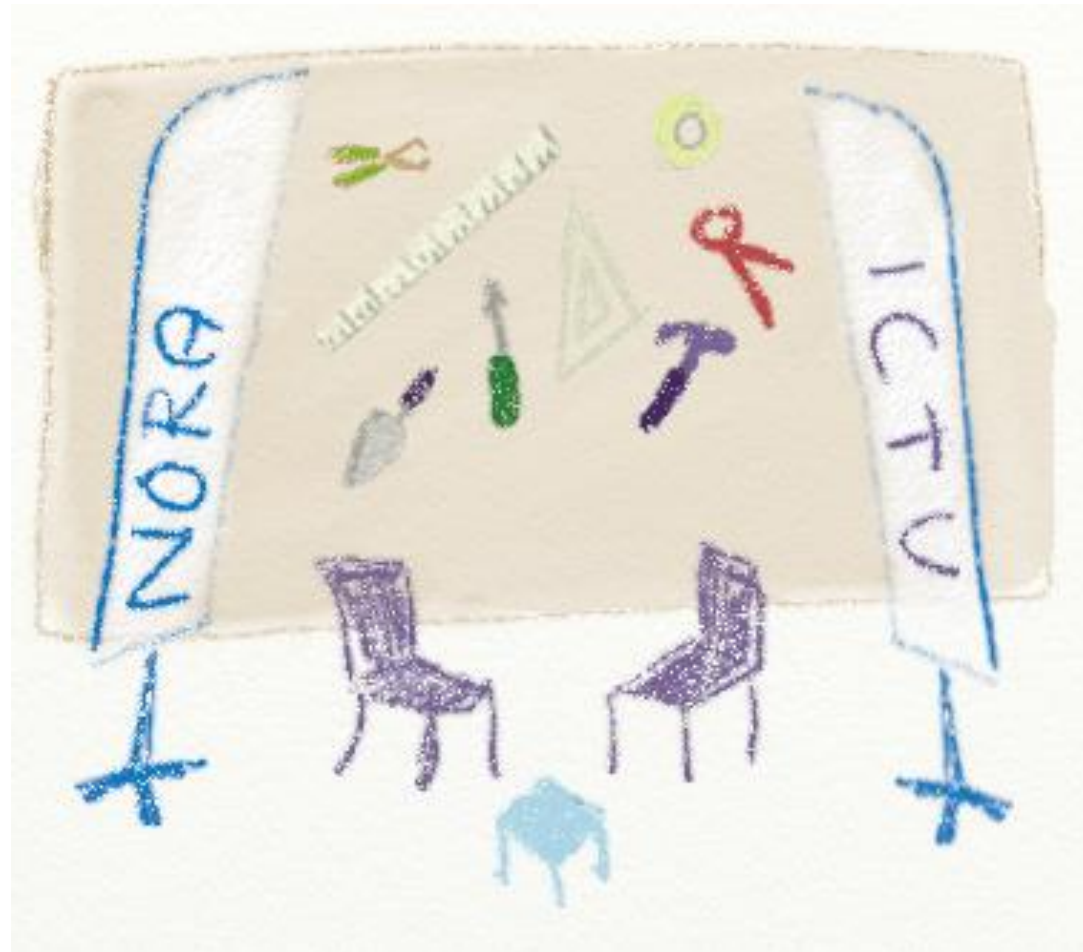
[NORA Beheer](#)

[@NORArchitectuur](#)

Deelname:

[NORA Gebruikersraad](#)

[Open Huis van de Architectuur](#)



Blijf op de hoogte:

[Nieuws & Agenda](#)

[Persoonlijke volglijst](#)

[NORA Familienieuws](#)

[RSS-feeds NORA](#)

Social media:

[X \(uitfaseren\)](#)

[LinkedIn](#)

[Mastodon \(binnenkort\)](#)

Sessies op DADD:

