Digital Architecture Design Day

NORA Familie: Bouw mee aan een veilige overheidsdienstverlening

5 oktober 2023

Marieke Vos, Guus van den Berg en Joris Dirks

NORA
Nederlandse Overheid
Referentie Architectuur

Wat is de NORA Familie?

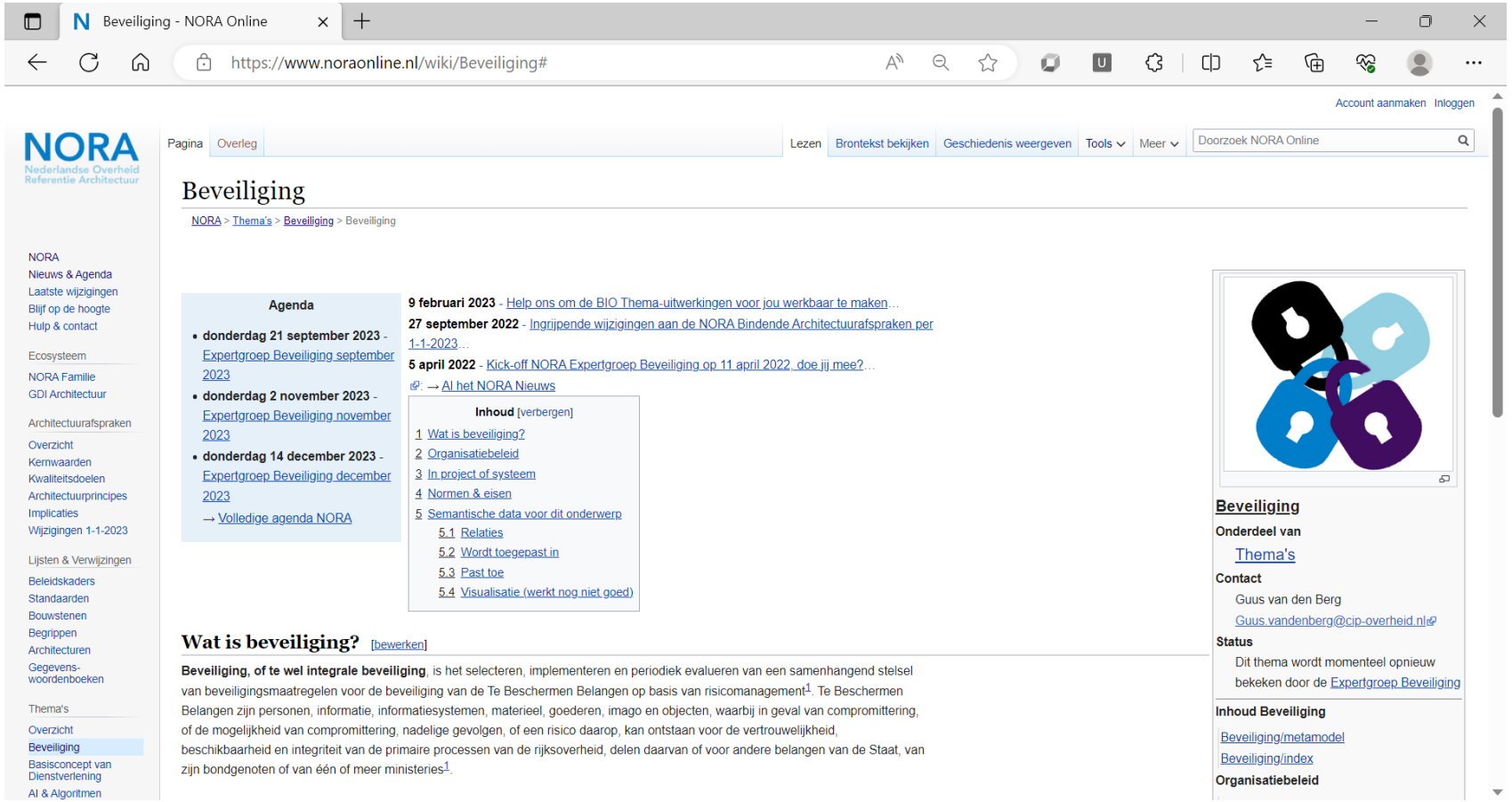
1. Kennis-community van architecten & architecturen in de publieke sector, met de wiki noraonline.nl als publiek kennisplatform
2. Inhoudelijk eigenaar van de NORA Kernwaarden van Dienstverlening, Kwaliteitsdoelen, Architectuurprincipes & Implicaties

NORA
Nederlandse Overheid
Referentie Architectuur

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



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?

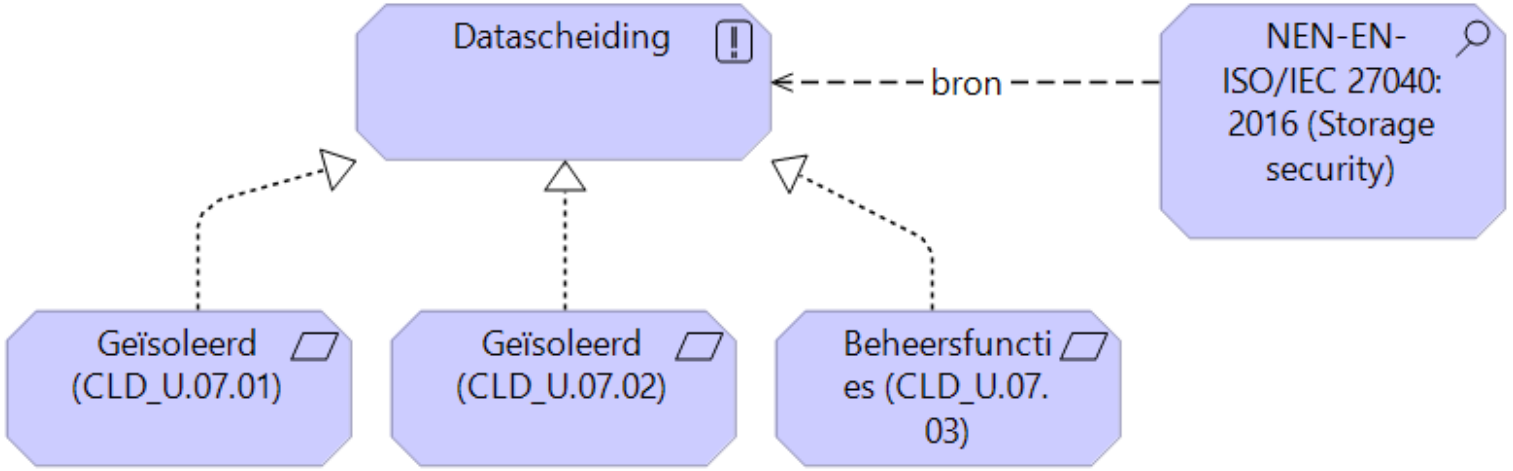
En is dat bruikbaar?

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…



- Thema
  - Gec
  - Ver
  - App

Datascheiding

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.

ISOR Beveiliging PRINCIPE

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

Indeling

Beveiligingsaspect: U — Uitvoering

Invalshoek: F — Functie

Verwante principes

→ BIO Thema-uitwerking Clouddiensten
→ Binnen dit normenkader èn beveiligingsaspect
→ Alle Normenkaders
→ Alle Beveiligingsprincipes
→ Alle Normen
→ Beveiligingsaspecten
→ ISOR

NEN-EN-ISO/IEC 27040: 2016 (Storage security)

NORA
Nederlandse Overheid Referentie Architectuur

Thema Beveiliging

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

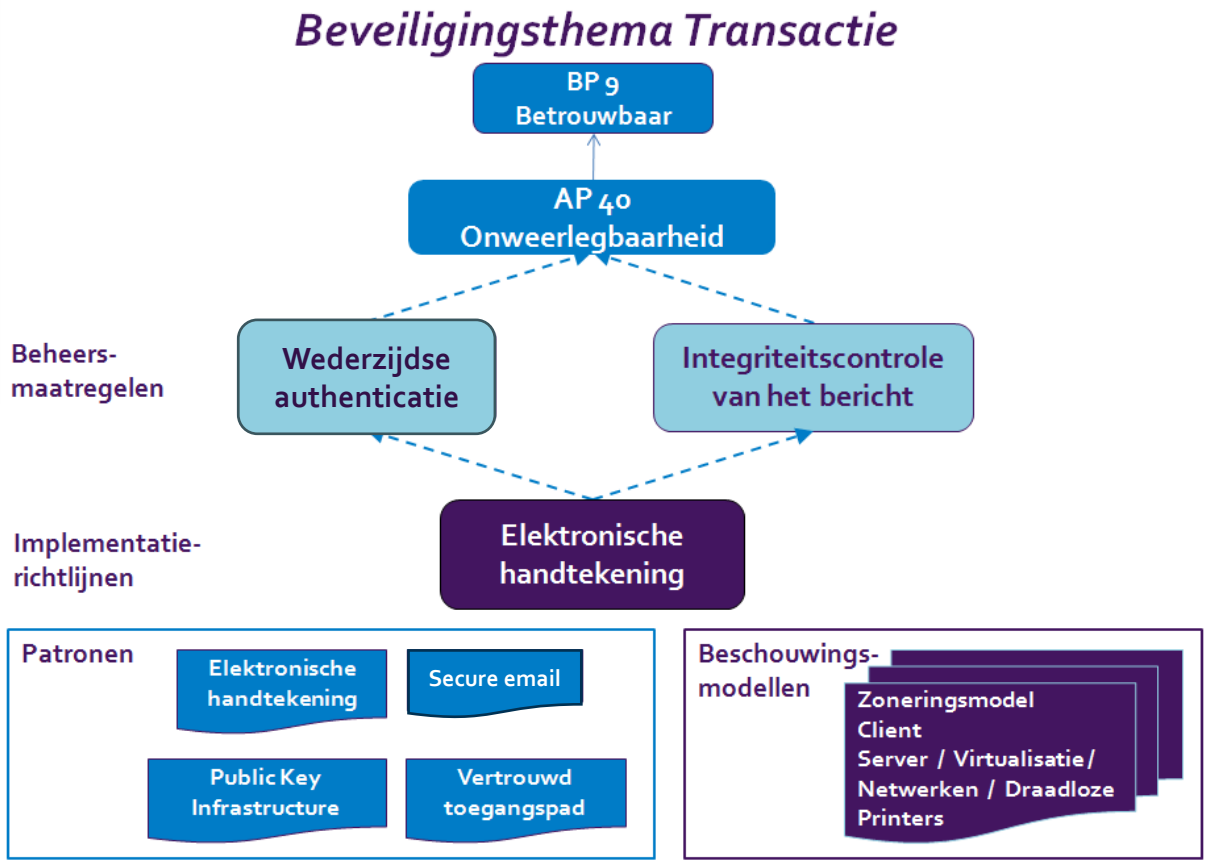
Beheersmaatregelen (2013)

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



Beheer

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

El
ha

Pub
Infras

ederzijdse 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))

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

NORA
Nederlandse Overheid
Referentie Architectuur

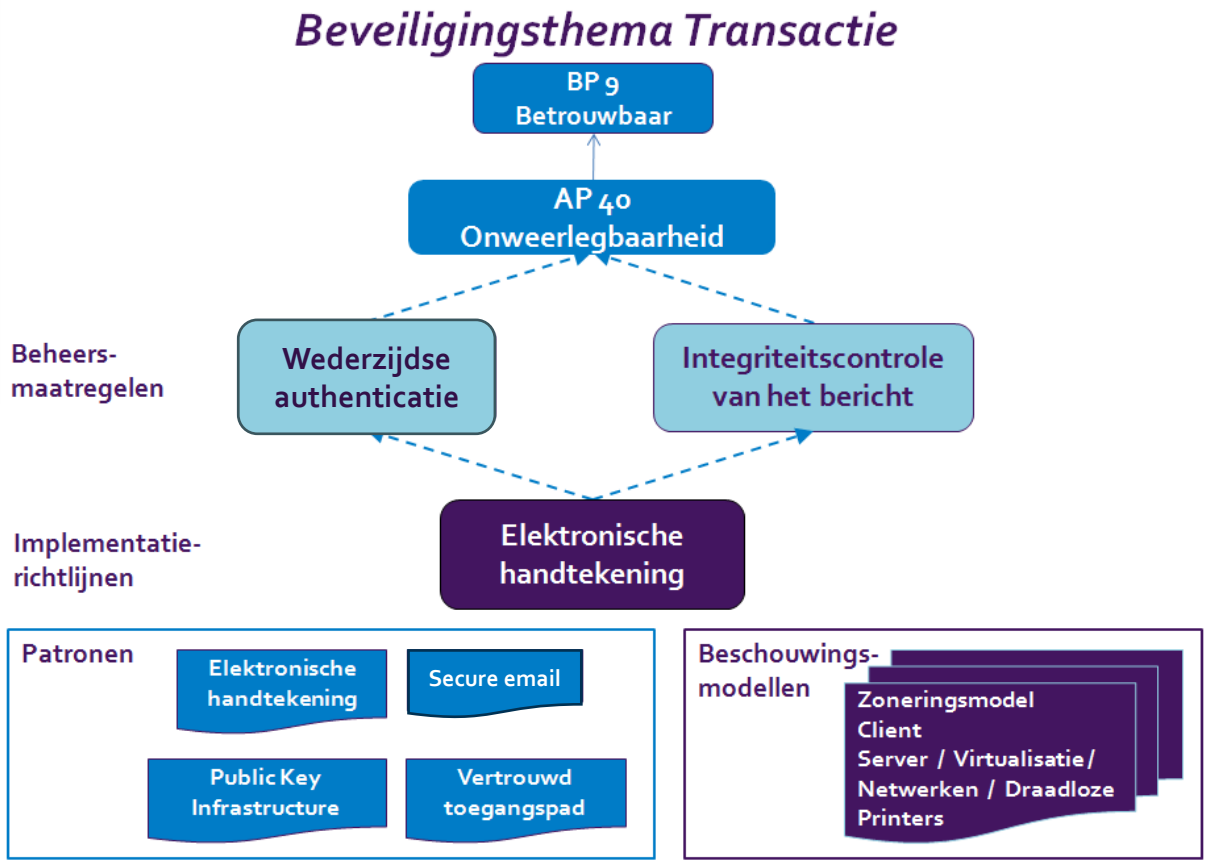
Patronen (2013)

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



Patr

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

Bevei

Beheers-
maatregelen

Wederzijd
authentic

Implementatie-
richtlijnen

Patronen

Elektronische handtekening

Public Key Infrastructure

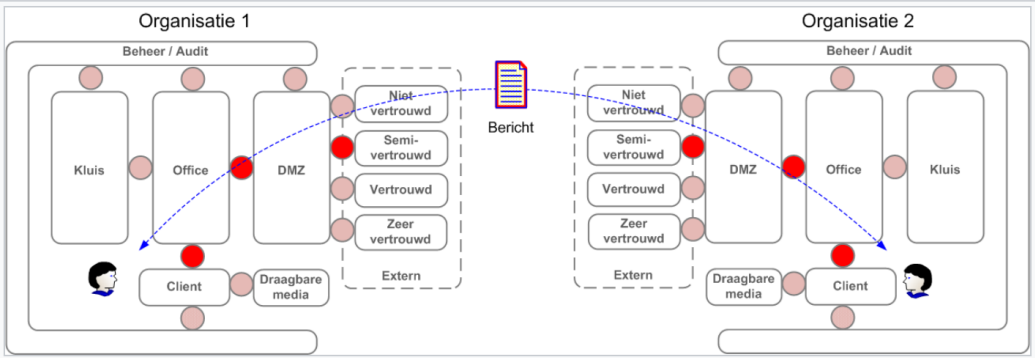
Patroon voor secure email

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.



Uitwisseling van elektronische berichten

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 verstuurd is
het bericht de geadresseerde heeft bereikt. De onweerlegbaarheid van de verzending en van de aankomst
tijdstippen daarvan is normaliter niet geregeld.

Oplossing [bewerken]

lossing is het beveiligen van het bericht voordat het de ver
bekend:

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?

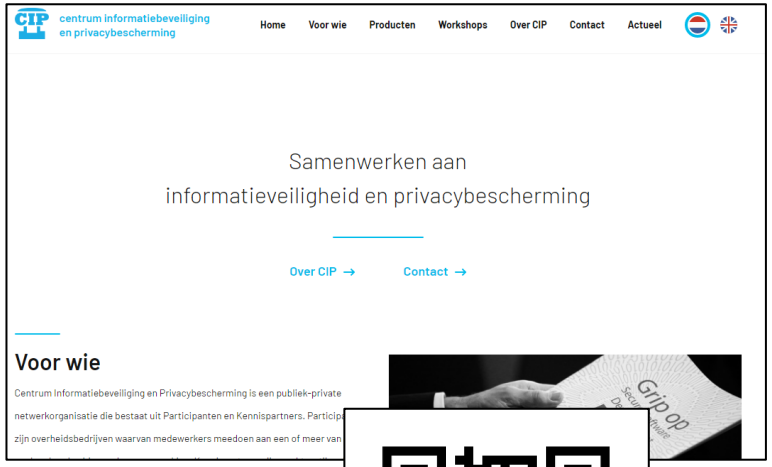
Meer informatie

[Beveiliging - NORA Online]

[Privacy - NORA Online]

CIP-community

CIP-website



CIP-YouTube kanaal

CIP-LinkedIn

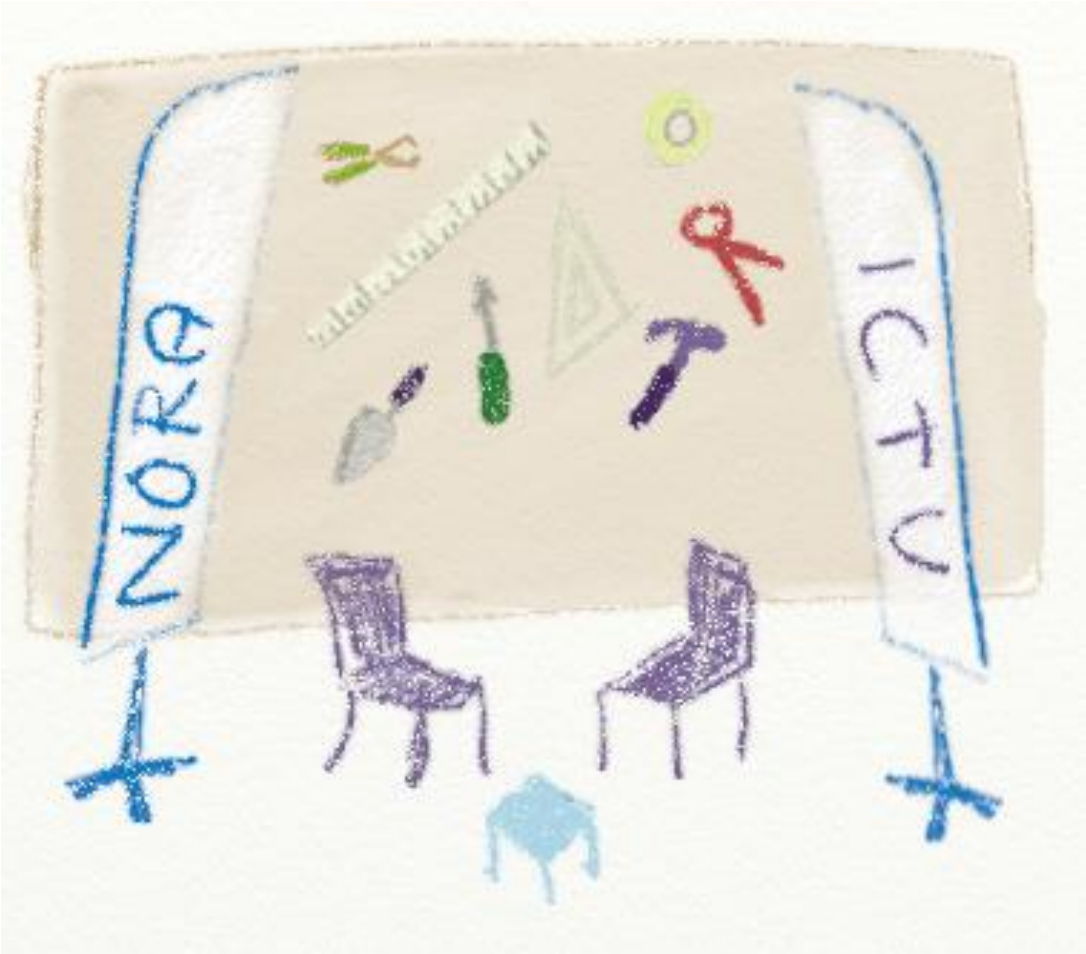
Schuif eens aan bij de NORA Familie

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:

NORA
Nederlandse Overheid
Referentie Architectuur