Kennisnet

ECK ID Voorschriften

SchoolID Services

Laat ict werken **voor het onderwijs**

Inhoud

Document informatie

Status

Auteur	Kennisnet, Marc Fleischeuers
Versie	0.2
Versiedatum	26 oktober 2017
Status	Goedgekeurd

Versiehistorie

Versie	Datum	Auteur	Beschrijving
0.1	20-10-2017	Vincent Tedjakusuma	Opgemaakt uit Technische voorschriften 1.0.10
0.2	26-10-2017	Marc Fleischeuers	Review en redactie

Distributie en goedkeuring

Versie	Datum	Goedgekeurd (indien van toepassing)

1. Voorschriften voor het verwerken van het ECK iD

In dit document worden de voorschriften rondom de beveiliging van het ketenpseudoniem beschreven dat gebruikt zal worden in de educatieve contentketen (ECK iD). Deze voorschriften zijn van toepassing op alle processen en partijen die het ECK iD verwerken en zijn noodzakelijk om te voldoen aan de afspraken vastgesteld in het Privacy Convenant. Deze voorschriften zijn overgenomen uit de “Technische voorschriften” voor de Nummervoorziening versie 1.0.10 van 15 maart 2017.

De hieronder genoemde maatregelen zijn de technische en organisatorische maatregelen om ervoor te zorgen dat de gepseudonimiseerde gegevens van leerlingen en docenten[1] niet aan de persoon zelf kunnen worden gekoppeld, tenzij hiervoor onredelijk zware middelen ingezet worden.

Met deze beveiligingsvoorschriften worden de volgende doelen gerealiseerd:

1. Voorschriften zijn gericht op voorkomen van onbevoegd gebruik en voorkomen van misbruik van het ECK ID
2. De gebruikte encryptie- en hashing-algoritmen worden breed toegepast in productiesystemen, zijn goed onderzocht en blijven voor de voorziene toekomst, 5 à 10 jaar, nog actueel[2]. Zie hiervoor met name voorschriften 2, 4, 5, 6 en 9 op pagina **Error! Bookmark not defined.** en verder.

De voorschriften worden beschreven aan de hand van de verwerkingen die plaats vinden tijdens het gebruik van het ECK iD.

De hier geformuleerde maatregelen op het gebied van encryptie zijn gebaseerd op “ICT richtlijnen voor Transport Layer Security”, Nationaal Cyber Security Centrum van het Ministerie van Justitie, “Gebruik en Achtergrond Digikoppeling Certificaten”, Logius, versie 1.2.1 (definitief), en “Algorithms, key size and parameters report - 2014”, European Union Agency for Network and Information Security (ENISA), november 2014. De aanbevelingen over sleutellengten en algoritmen uit het ENISA rapport komen overeen met diverse andere aanbevelingen van Europese en Amerikaanse[3] agentschappen.

1.1. *Voorschrift ECKID-1*: Basis voor stampseudoniem van docenten.

Docenten beschikken niet over een PGN en het is niet wenselijk om het BSN te gebruiken als basis voor het stampseudoniem. Bovendien is de situatie voor docenten anders dan voor leerlingen, zodat ook de eisen aan het pseudoniem anders worden. Docenten zijn in het algemeen actief in de educatieve leermiddelenketen vanwege hun aanstelling bij een specifieke school of bestuur.[4] De school beschikt over de licenties van materialen en toegang tot systemen voor onderwijs en -ondersteuning. De basis voor het stampseudoniem van een docent zal dan ook een uniek kenmerk zijn van de docent *binnen de school of bestuur*. Uitgangspunt voor het bepalen van een stampseudoniem voor een docent is dan ook dat als een docent werkzaam is voor meerdere besturen (en daarmee op meerdere scholen), dat de docent voor elk bestuur een apart, ongerelateerd stampseudoniem beschikt.

Naast uniciteit kan *stabiliteit* ook een gewenste eigenschap zijn van het kenmerk van docenten. Normaal gesproken wordt een stampseudoniem maar een keer gedurende de aanstelling van een docent op school aangevraagd, maar het kan zijn dat een school overstapt op een nieuw administratief systeem waardoor de stampseudoniemen van alle docenten opnieuw moet worden aangemaakt, of dat gegevens in de administratie verloren zijn gegaan. In deze situatie moet de docent weer kunnen beschikken over hetzelfde stampseudoniem en alle daarvan afgeleide ketenpseudoniemen. De werkwijze die we hiervoor hanteren is om de GUID die de basis is voor het stampseudoniem van de docent (zie hieronder) te migreren naar het nieuwe administratieve

[1] Leerlingen en docenten zijn hier bedoeld als alle onderwijsvolgers en medewerkers van onderwijsinstellingen.

[2] “Algorithms, key size and parameters report – 2014”, European Union Agency for Network and Information Security (ENISA), 2014

[3] Het Information Assurance Directorate van het NSA heeft voor een specifieke, beperkte groep commercieel verkrijgbare pakketsoftware met encryptiefunctionaliteit bepaald dat deze alleen met een vergunning geëxporteerd mag worden. Voor de hier besproken algoritmes geldt in het algemeen dat ze niet onder deze bepaling vallen. Zie http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear en http://www.bis.doc.gov/index.php/forms-documents/doc_download/951-ccl5-pt2

[4] Scholen kunnen hiërarchisch georganiseerd zijn onder een schoolbestuur. We gaan er hierbij van uit dat een docent dezelfde rechten en mogelijkheden heeft op alle scholen onder een bestuur.

systeem, of te herstellen vanuit een backup in het geval van gegevensverlies. Hiermee wordt voor een docent in alle gevallen dezelfde werkwijze om pseudoniemen te maken en herstellen gebruikt als voor leerlingen.

Als basis voor het pseudoniem van een docent wordt een GUID te gebruikt, en wel als volgt:

- Gebruik GUIDs volgens rfc 4122 (https://www.ietf.org/rfc/rfc4122.txt)
- Gebruik een GUID van type 1 (gebaseerd op tijdstip) of type 4 (random)
- Gebruik de urn: representatie van de GUID, bijv. urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
- Neem maatregelen zodat de GUID beschikbaar is voor herstel van verloren pseudoniemen in de administratie en voor migratie van pseudoniemen in geval van migratie naar een nieuw administratiesysteem

Deze werkwijze levert een tekenreeks op, die net als het PGN voor leerlingen gehasht wordt volgens *voorschrift 2* voordat het wordt aangeboden aan de Nummervoorziening.

1.2. *Voorschrift ECKID-2*: Opslag van het stampseudoniem en ketenpseudoniem in de administratieve omgeving van de school

Een schooladministratie beschikt over gevoelige persoonsgegevens en heeft maatregelen genomen tegen onbevoegd gebruik en misbruik van deze gegevens. Opslag van het stampseudoniem en ketenpseudoniem wordt onder dezelfde maatregelen gedaan. Dit voorschrift beschrijft de eisen aan *persistente* opslag van het stam- en ketenpseudoniem in de schooladministratie. De schooladministratie is hierbij het geheel aan administratieve applicaties (bijv. LAS, LVS, authenticatiesysteem) waarmee de instelling de gegevens van zijn leerlingen (en naar verwachting ook de pseudoniemen van docenten) beheert.

In de privacy impact analyse van de Nummervoorziening is een risico gesignaleerd dat leerlinggegevens over partijen heen (onrechtmatig) gekoppeld zouden kunnen worden. Hierbij ontstaan grotere verzamelingen met persoonsgegevens. Als algemene maatregel tegen dit risico wordt het volgende voorgesteld:

> *Voor wat informatiebeveiliging en eventuele datalekken betreft, wordt, weliswaar ter afsluiting van de PIA maar wel degelijk essentieel, aanbevolen om het ketenpseudoniem en het PGN op geëncrypte wijze vast te leggen in de systemen van de scholen en met name in de leerlingenadministratiesystemen en andere systemen waarin zowel het PGN, personalia en het ketenpseudoniem vastgelegd zijn. Een dergelijke beveiligingsmaatregel past bijvoorbeeld bij de inmiddels gebruikelijke handelwijze dat ook gebruikersnamen en wachtwoorden geëncrypt vastgelegd worden. (Privacy Impact Assessment Nummervoorziening in de Leermiddelenketen, PBLQ, p. 43)*

Doel hiervan is te zorgen dat met onrechtmatig verkregen gegevens van een of meer registraties uit een andere organisatie er geen koppeling met andere registraties gemaakt kan worden. Het niet kunnen herleiden van personen na koppeling van gegevens is ook in de AVG opgenomen als belangrijke eigenschap van goede pseudonimisering.

De aanbevelingen voor implementatie die de PIA geeft, nemen we over ter referentie. Als leveranciers alternatieve implementaties willen gebruiken dienen zij aan te tonen dat ze een zelfde niveau van bescherming kunnen bieden tegen het hierboven genoemde risico op onrechtmatige koppeling.

- Partijen gebruiken ECK ID's in communicatie met externe partijen in de leermiddelenketen.
- Stampseudoniemen worden nooit gebruikt in communicatie tenzij bij het aanvragen van ketenpseudoniemen bij de Nummervoorziening.
- Partijen gebruiken stampseudoniemen en ketenpseudoniemen niet als interne identificatie van leerlingen of docenten.
- Bij de opslag van het stampseudoniem en ketenpseudoniem in administraties wordt encryptie toegepast.
- Elke partij past zijn eigen encryptie toe (die voldoet aan de minimumvoorschriften, zie verderop), zodat er geen koppelrisico voor gegevens over leveranciers heen ontstaat

De gewenste scheiding tussen gegevens is een *logische* scheiding, die ontstaat doordat de opgeslagen pseudoniemen niet herleidbaar zijn zonder toegang tot de encryptiesleutel. Hier hoort bij dat de opslag van de private encryptiesleutel voldoet aan de volgende maatregel:

- Private encryptiesleutels worden opgeslagen met de meest minimale set aan toegangsrechten mogelijk: alleen leestoegang voor het serviceaccount dat gebruikt wordt om een ver- of ontsleutelingsoperatie uit te voeren; toegang tot dit account is beperkt en wordt gelogd

De eisen die aan de encryptie worden gesteld zijn geformuleerd in “Algorithms, key size and parameters report – 2014”, European Union Agency for Network and Information Security (ENISA), 2014:

- Gebruikte encryptie algoritmen zijn bewezen veilig
- Gebruikte sleutellengten zijn 128-bits (symmetrisch) of meer
- Algoritmen hebben geen structurele zwakheden
- Algoritmen zijn uitvoerig bestudeerd en gestandaardiseerd

Voorbeelden van encryptiealgoritmen die hieraan voldoen zijn AES en Camellia. Voorbeelden van algoritmen die alleen nog in legacy situaties (niet voor nieuwbouw) gebruikt kunnen worden zijn 3DES en Blowfish. Een onveilig algoritme dat niet meer mag worden gebruikt is DES encryptie.

1.3. *Voorschrift ECKID-3*: Opslag van het ECK ID bij de ketenpartij

Dit voorschrift beschrijft de eisen aan *persistente* opslag van ketenpseudoniemen in de administratie van ketenpartijen. De administratie is hierbij het geheel aan administratieve applicaties waarmee de partij de gegevens van zijn gebruikers (leerlingen en docenten) beheert.

Doel van dit voorschrift is te zorgen dat met onrechtmatig verkregen gegevens van een of meer registraties uit een andere partij er geen koppeling met andere registraties gemaakt kan worden. Het niet kunnen herleiden van personen na koppeling van gegevens is ook in de AVG opgenomen als belangrijke eigenschap van goede pseudonimisering.

De aanbevelingen voor implementatie die de PIA geeft, nemen we over ter referentie. Als ketenpartijen alternatieve implementaties willen gebruiken dienen zij aan te tonen dat ze een zelfde niveau van bescherming kunnen bieden tegen het hierboven genoemde risico op onrechtmatige koppeling.

- Partijen gebruiken ECK ID's in communicatie met externe partijen in de leermiddelenketen.
- Partijen gebruiken ketenpseudoniemen niet als interne identificatie van leerlingen of docenten.
- Bij de opslag van ketenpseudoniemen in administraties wordt versleuteling (encryptie of hashing, zie verderop) toegepast.
- Elke partij past zijn eigen versleuteling toe (die voldoet aan de minimumvoorschriften, zie verderop), zodat er geen koppelrisico voor gegevens over leveranciers heen ontstaat

De gewenste scheiding tussen gegevens is een *logische* scheiding, die ontstaat doordat de opgeslagen pseudoniemen niet herleidbaar zijn zonder toegang tot de encryptiesleutel en / of het gebruikte salt. Hier hoort bij dat de opslag van de private encryptiesleutel of salt voldoet aan de volgende maatregel:

- Private encryptiesleutels en / of salts worden opgeslagen met de meest minimale set aan toegangsrechten mogelijk: alleen leestoegang voor het serviceaccount dat gebruikt wordt om een ver- of ontsleutelingsoperatie uit te voeren; toegang tot dit account is beperkt en wordt gelogd

1.3.1. Keuze van versleuteling

Voor de keuze van versleuteling die de ketenpartij toepast, is het van belang op welke manier de partij communiceert in de keten. We onderscheiden hierbij twee situaties:

1. De ketenpartij wisselt gegevens van individuele leerlingen uit met de school of andere ketenpartij, ook buiten de gebruikerssessie van de ingelogde leerling.

2. De ketenpartij wisselt *geen* gegevens van individuele leerlingen uit met school of andere ketenpartij.

Partijen waarvoor situatie 1 geldt, gebruiken een omkeerbare versleuteling (encryptie) bij de opslag van het ketenpseudoniem. Partijen waarvoor situatie 2 geldt, gebruiken een niet-omkeerbare versleuteling (hashing) voor de opslag van het ketenpseudoniem.

1.3.2. Eisen aan encryptie

De eisen die gesteld worden aan encryptie zijn dezelfde die gesteld worden volgend *voorschrift 5*:

- Gebruikte encryptie algoritmen zijn bewezen veilig
- Gebruikte sleutellengten zijn 128-bits (symmetrisch) of meer
- Algoritmen hebben geen structurele zwakheden
- Algoritmen zijn uitvoerig bestudeerd en gestandaardiseerd

Voorbeelden van encryptiealgoritmen die hieraan voldoen zijn AES en Camellia. Voorbeelden van algoritmen die alleen nog in legacy situaties (niet voor nieuwbouw) gebruikt kunnen worden zijn 3DES en Blowfish. Een onveilig algoritme dat niet meer mag worden gebruikt is DES encryptie.

1.3.3. Eisen aan hashing

De eisen die gesteld worden aan de gebruikte hashingalgoritme zijn

- Elke partij kiest een eigen hashingalgoritme met bijbehorend salt, dat voldoet aan de minimumvoorschriften, zodat er geen koppelrisico voor gegevens over partijen heen ontstaat
- De ketenpartner kiest een hashfunctie die voldoet aan de eisen uit het ENISA rapport en dat hashes van 256 bits of meer produceert.

Voorbeelden van algoritmen die voldoen zijn algoritmen uit de SHA-2 familie, SHA3 en Whirlpool. Algoritmes die niet mogen worden gebruikt zijn SHA-1, RIPEMD en MD-5, vanwege een te korte outputlengte of andere zwakheden.

De gewenste scheiding tussen gegevens is een *logische* scheiding, die ontstaat doordat de opgeslagen pseudoniemen niet herleidbaar zijn zonder toegang tot het gebruikte salt. Hier hoort bij dat de opslag van het salt voldoet aan de volgende maatregel:

- Salts worden opgeslagen met de meest minimale set aan toegangsrechten mogelijk: alleen leestoegang voor het serviceaccount dat gebruikt wordt om de hashingoperatie uit te voeren; toegang tot dit account is beperkt en wordt gelogd

1.4. *Voorschrift ECKID-4*: Toepassen van TLS tussen browser en ketenpartner

Dit voorschrift wordt toegepast voor verbindingen van browsers van gebruikers (op school en daarbuiten, vanaf laptop en mobiele devices). Dit voorschrift verschilt van *voorschrift 7* omdat er minder controle is over de client (browser in plaats van LAS).

Hiervoor wordt het gebruiksadvies van de ICT-beveiligingsvoorschriften van het NCSC gevolgd voor het scenario waarin alleen controle is over de server. Dit betreft dus een maatregel die ketenpartijen implementeren in hun servers. Op http://www.ssllabs.com/ssltest/client.html staat een overzicht van alle configuraties die ondersteund worden door clients.

- Gebruik alleen TLS versie 1.2, 1.1 of 1.0 (in volgorde van afnemende voorkeur)
- Kies GOEDE en VOLDOENDE cyphersuites voor de server. Ondersteun niet meer cyphersuites dan alleen deze GOEDE en VOLDOENDE suites. Zie de ICT-beveiligingsvoorschriften van het NCSC voor een uitputtende lijst.

- Kies voldoende lengte van parameters en sleutels. Zie de ICT-beveiligingsvoorschriften van het NCSC voor aanbevelingen.

Verificatie van de instellingen van de servers kan plaatsvinden met behulp van de SSL Server test van Qualys, https://casecurity.ssllabs.com/.

1.5. *Voorschrift ECKID-5*: Toepassen van TLS tussen administratieve omgevingen van school

Dit voorschrift wordt toegepast als stam- en / of ketenpseudoniemen getransporteerd worden via systeem – systeem koppelingen binnen een (onderwijs)organisatie, in situaties waarbij de koppeling over het publieke internet zonder additionele veiligheidsmaatregelen (bijvoorbeeld ssh- of vpn-tunnel met voldoende zware encryptie). Denk hierbij bijvoorbeeld aan leerlingadministraties of -portalen ondergebracht bij cloud-providers, waarbij alle gegevensverkeer verloopt over het publieke internet.

Voor deze verbindingen geldt dat het gebruiksadvies van de ICT-beveiligingsvoorschriften van het NCSC voor het scenario waarin controle is over client en server wordt gevolgd. Voor deze koppeling wordt gebruik gemaakt van beveiliging op transport-niveau met deze eigenschappen:

- Gebruik alleen TLS versie 1.2 of hoger.
- Kies GOEDE cyphersuites voor de server. Ondersteun niet meer cyphersuites dan alleen deze GOEDE suites. Zie de ICT-beveiligingsvoorschriften van het NCSC voor een uitputtende lijst.
- Kies voldoende lengte van parameters en sleutels. Zie de ICT-beveiligingsvoorschriften van het NCSC voor aanbevelingen.

Edukoppeling 1.2 voldoet aan dit voorschrift, dus als de koppeling aangelegd kan worden met Edukoppeling 1.2 of hogere versie, dan voldoet deze koppeling aan het voorschrift.