Kennisnet

ECK ID Technische voorschriften

SchoolID Services

Laat ict werken **voor het onderwijs**

Inhoud

DOCUMENT INFORMATIE 2

Status 2

Versiehistorie 2

Betrokken/geraadpleegd 2

Distributie en goedkeuring 2

1. SAMENVATTING 3

2. TECHNISCHE VOORSCHRIFTEN 4

2.1. Voorschrift *1*: Basis voor ECK ID van docenten 4

2.2. *Voorschrift 2*: 1e niveau hashing van basis ECK ID 5

2.3. *Voorschrift 3*: Toepassen van EduKoppeling 5

2.4. *Voorschrift 4*: De hashing van de Nummervoorziening 6

2.5. *Voorschrift 5*: Opslag van het ECK ID bij de leerlingadministratie 6

2.6. *Voorschrift 6*: Opslag van het ECK ID bij de ketenpartij 7

2.7. *Voorschrift 7*: Toepassen van TLS tussen LAS en Nummervoorziening 7

2.8. *Voorschrift 8*: toepassen van TLS tussen browser en ketenpartner 8

Document informatie

Status

Auteur	Kennisnet, Marc Fleischeuers
Versie	0.92
Versiedatum	mei 2016
Status	Concept

Versiehistorie

Versie	Datum	Auteur	Beschrijving
0.9	6 april 2016	Marc Fleischeuers	Samengesteld uit eerdere documenten
0.91	18 april 2016	Marc Fleischeuers	Naar aanleiding van Edu-K KAT overleg
0.92	11 mei 2016	Marc Fleischeuers	Encryptieeisen VS, Voorschriften 5 en 6 verder toegelicht, voorschrift 1 uitgewerkt

Betrokken/geraadpleegd

Betrokken	Rol

Distributie en goedkeuring

Versie	Datum	Persoon	Goedgekeurd (indien van toepassing)

1. Samenvatting

2. Technische voorschriften

In dit hoofdstuk worden de maatregelen rondom de beveiliging beschreven van het ketenpseudoniem dat gebruikt zal worden in de educatieve leermiddelenketen (ECK ID). Met deze beveiligingsmaatregelen worden de volgende doelen gerealiseerd:

1. ECK IDs voor leerlingen van het PO, VO, MBO zijn blijvend uniek binnen het onderwijs.
2. ECK IDs voor leerlingen van het PO, VO, MBO zijn persistent gedurende tenminste het verblijf van de leerling in een onderwijssector.
3. ECK IDs zijn niet direct herleidbaar tot de persoon en geven geen informatie over de persoon.
4. Maatregelen zijn gericht op voorkomen van onbevoegd gebruik en voorkomen van misbruik van het ECK ID
5. 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[1]. Zie hiervoor met name voorschriften 2, 4, 5, en 6 op pagina 5 en verder.

De maatregelen worden beschreven aan de hand van de verwerkingen die plaats vinden tijdens het aanmaken en gebruik van het ECK ID. Een en ander is geïllustreerd aan de hand van de basis use case “Genereer een ECK ID” in het document “Principes en processen”.

Deze maatregelen zijn nu specifiek voor dit project, terwijl ze feitelijk generiek van aard zijn (bijvoorbeeld de beveiliging van gegevens en transportkanalen). Het is de intentie om de projectspecifieke maatregelen te vervangen door bredere kaders zoals Edukoppeling en het Certificeringsschema, zodra deze voldoende compleet en volwassen zijn. De hier geformuleerde maatregelen 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[2] agentschappen.

2.1. Voorschrift *1*: Basis voor ECK ID van docenten.

Docenten zijn in het algemeen actief in de educatieve leermiddelenketen vanwege hun aanstelling bij een specifieke school of bestuur.[3] De school beschikt over de licenties van materialen en toegang tot systemen voor onderwijs en -ondersteuning. De basis voor het ECK ID van een docent zal dan ook een uniek kenmerk zijn van de docent binnen de school of bestuur.

Naast uniciteit kan *stabiliteit* ook een gewenste eigenschap zijn van het kenmerk van docenten. Normaal gesproken wordt een ECK ID maar een keer in de carrière van een docent op school aangevraagd, maar het kan zijn dat een school overstapt op een nieuw administratief systeem waardoor de ECK IDs van alle docenten opnieuw moet worden aangemaakt. In deze situatie moet de docent weer kunnen beschikken over hetzelfde ECK ID, en dat kan door ofwel het ECK ID te migreren naar het nieuwe systeem, of door het opnieuw, op basis van hetzelfde kenmerk, aan te vragen bij de Nummervoorziening. In de laatste situatie is stabiliteit van het kenmerk relevant.

In Edu-K verband zijn een drietal methoden genoemd waarmee een basis voor het ECK ID voor docenten kan worden gevormd. Elk van deze methoden voldoet aan de wens voor stabiliteit en uniciteit zoals hierboven genoemd. LASsen bieden scholen de keuze uit deze werkwijzen, en een school kiest de werkwijze die het best past in zijn situatie.

---

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

[2] 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

[3] 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.

De werkwijzen zijn

- Gebruik een combinatie van (een school-specifiek) emailadres van de docent en het nummer van het bestuur waar de school onder valt. Overweeg deze werkwijze alleen als het deel voor de '@' in het emailadres tenminste 8 letters of cijfers bevat.
- Gebruik het docent-nummer van de docent in het LAS in combinatie met het nummer van het bestuur; overweeg dit alleen als het docentnummer tenminste 8 letters of cijfers bevat.
- Gebruik een random GUID en zorg ervoor dat het ECK ID van de docenten gemigreerd kan worden als het systeem de ECK IDs registreert wijzigt (bijvoorbeeld als de school overgaat naar een nieuw LAS).

In alle gevallen geldt dat de werkwijze een tekenreeks oplevert, die net als het PGN voor leerlingen gehasht wordt volgens *voorschrift 2* voordat het wordt aangeboden aan de Nummervoorziening.

2.2. *Voorschrift 2*: 1e niveau hashing van basis ECK ID

Hiervoor wordt gebruik gemaakt van scrypt. Deze functie heeft een aantal parameters waarmee de zwaarte van het berekenen van de hash wordt gestuurd. De zwaarte is zodanig gekozen dat het normale werk, het aanvragen van een ECK ID bij de aanmelding van een leerling, niet wordt gehinderd terwijl het misbruik (aanleg van een vertaaltabel) wordt ontmoedigd.

Op basis van overwegingen dat de 1e niveau hashing server-side wordt toegepast (dwz in een omgeving waar veel geheugen aanwezig is) worden deze parameters gebruikt:

Parameter	Waarde	Toelichting
N	2^{17} = 131072	Bepaalt wat het geheugenbeslag van de individuele operaties gaat zijn.
r	8	Factor voor geheugenbeslag.
p	4	Parameter voor parallelle verwerking en dus voor de tijd die de berekening gaat kosten.

Figuur 1 Voorgeschreven parameters voor scrypt

Met deze parameters zal het geheugenbeslag voor de aanvraag van een ECK ID ongeveer 130MB en duurt op een core i5 (single core) ongeveer 10 seconden. In het originele paper van scrypt (http://www.tarsnap.com/scrypt/scrypt.pdf) wordt geadviseerd om N = 2^{14} of N = 2^{16} te kiezen. Voor normaal gebruik op client systemen (PC, laptop) zijn dit nog steeds veel gebruikte waarden. Voor de server-omgeving waarin deze functie wordt gebruikt geldt dat deze meer geheugen en meer CPU cores beschikbaar heeft, vandaar de iets zwaardere parameters.

Nota bene: er zijn scrypt bibliotheken die de gekozen parameters opnemen in de output. Voor verwerking in de Nummervoorziening dient *alleen* de hashwaarde te worden gebruikt, uitdrukkelijk zonder deze parameters.

De uitvoer van de scrypt functie, de hash, is een getal van 128 bits. Dit getal wordt voor onderlinge uitwisseling geconverteerd naar een 32 karakters lange hexadecimale string.

2.3. *Voorschrift 3*: Toepassen van EduKoppeling.

Edukoppeling wordt toegepast voor server-naar-server communicatie tussen leerlingadministratie client en Nummervoorziening. Hiervoor geldt:

a. Er wordt gebruik gemaakt van EduKoppeling 1.2 of een latere, door de Standaardisatieraad vastgestelde versie.

b. Het gebruikte certificaat van de service client bevat het OIN van de leerlingadministratie-leverancier en is verkregen bij een Digikoppeling CSP.

c. Partijen die dienst afnemen hebben de plicht om hun certificaat in te laten trekken indien dit niet meer gebruikt wordt of gecompromitteerd is.

d. De WS-Addressing headers van het bericht bevatten OINs van onderwijsinstelling en de Nummervoorziening. Het OIN van de onderwijsinstelling[4] is samengesteld als “00000007000” + BRIN (4 pos) + Administratienummer (5 pos).

e. Het bericht is 2W-BE, en niet ondertekend en niet encypted.

2.4. *Voorschrift 4*: De hashing van de Nummervoorziening.

Hiervoor wordt gebruik gemaakt van SHA-512 hash algoritme. Dit algoritme maakt een hash van 512 bytes output. Deze waarde wordt gezien als toekomstvast en wordt aangeraden in het rapport “Algorithms, key size and parameters report – 2014”, European Union Agency for Network and Information Security (ENISA), 2014. In het Afsprakenstelsel eHerkenning wordt gesteld dat een pseudoniem een hexadecimale string van 32 karakters is, dat wil zeggen 128 bits. Dit is een tamelijk korte sleutel en niet heel toekomstvast. Om deze reden wordt gekozen om een langere sleutel (512 bits, 128 hexadecimaal karakters) te gebruiken.

Voor communicatie converteert de nummervoorziening de hashwaarde naar een 128 karakters lange hexadecimale letterreeks.

De gebruikte salt-waarden wordt veilig en duurzaam opgeslagen met de minimale set aan toegangsrechten: alleen leestoegang voor het serviceaccount dat gebruikt wordt om de hashingoperatie uit te voeren.

2.5. *Voorschrift 5*: Opslag van het ECK ID bij de leerlingadministratie

Een leerlingadministratie beschikt al over gevoelige persoonsgegevens en heeft maatregelen genomen tegen onbevoegd gebruik en misbruik van deze gegevens. Opslag van het ECK ID wordt onder dezelfde maatregelen gedaan. Dit voorschrift beschrijft de eisen aan *persistente* opslag van het ECK ID in de leerlingadministratie. De leerlingadministratie is hierbij het geheel aan administratieve applicaties (bijv LAS, LVS, authenticatiesysteem) waarmee de instelling de gegevens van zijn leerlingen 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 van een ketenpartner er geen koppeling met andere registraties gemaakt kan worden.

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.

- Bij de opslag van het ECK ID in leerlingadministraties wordt encryptie toegepast
- Elke leverancier 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 ECK IDs niet interpreteerbaar zijn zonder toegang tot de encryptiesleutel. Hier hoort bij dat de opslag van de private encryptiesleutel voldoet aan de volgende maatregel:

[4] Het OIN is in Digikoppeling gedefinieerd als numeriek veld. Een BRIN bevat twee letters, daarom is het in de educatieve sector gebruikelijk om het OIN als alfanumeriek te gebruiken.

- Ontvangen en gegenereerde sleutels 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

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.

2.6. *Voorschrift 6*: Opslag van het ECK ID bij de ketenpartij

Met dit voorschrift is opslag van het ECK ID beschermd tegen ongeautoriseerd gebruik en tegen koppelen van persoonsgegevens over verschillende systemen. De maatregel uit dit voorschrift is ontleend aan het ENISA rapport.

In de meeste gevallen is het initiatief voor een gegevensuitwisseling met een ketenpartij afkomstig van de school, dat wil zeggen, een leerling of docent voert een actie uit (klikt op een link) in een schoolomgeving en wordt daarmee naar een systeem van de ketenpartij geleid. Als alle interactiepatronen die een ketenpartij heeft hiermee beschreven kunnen worden, zal de ketenpartij het ECK ID hashen voordat het in zijn systemen wordt opgeslagen, volgens de richtlijnen zoals hieronder beschreven. De opslag betreft hierbij *persistente* opslag.

Als het daarentegen voorkomt dat een ketenpartij spontaan berichten verstrekt en in deze berichten ECK IDs gebruikt, dan is het noodzakelijk dat de ketenpartij het ECK ID geencrypt opslaat (en dus ook gedecrypt kan worden om opgenomen te worden in het bericht). In dat geval voldoet deze opslag aan *voorschrift 5*.

Voor ketenpartners die de ECK IDs niet gebruiken in spontane berichten geldt:

- Bij de opslag van het ECK ID in het systeem van de partner wordt hashing toegepast
- Elke leverancier kiest een eigen hashingalgoritme met bijbehorend salt (dat voldoet aan de minimumvoorschriften, zie verderop), zodat er geen koppelrisico voor gegevens over leveranciers heen ontstaat
- De ketenpartner kiest een hashfunctie die voldoet aan de eisen uit het ENISA rapport, die 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.
- Indien een salt wordt gebruikt voor de hashing, dan wordt deze salt opgeslagen met de meest minimale set aan toegangsrechten mogelijk: alleen leestoegang voor het serviceaccount dat gebruikt wordt om de hashingoperatie uit te voeren.

2.7. *Voorschrift 7*: Toepassen van TLS tussen LAS en Nummervoorziening

Dit voorschrift wordt toegepast voor systeem – systeem verbindingen zoals tussen LAS en de Nummervoorziening. Voor deze verbindingen geldt dat er voorschriften aan zowel de client (LAS) als de server kunnen worden opgelegd. Hiervoor wordt het gebruiksadvies van de ICT-beveiligingsvoorschriften van het NCSC gevolgd voor het scenario waarin controle is over client en server. Dit betreft dus maatregelen die de Nummervoorziening zelf implementeert en maatregelen die ketenpartijen implementeren in hun client.

- Gebruik alleen TLS versie 1.2
- 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.

2.8. *Voorschrift 8*: 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/.