ZorgTTP
Privacy & vertrouwen

Methodebeschrijving TRES

ZorgTTP
De Bouw 127
3991 SZ Houten
Telefoon: 030-6360649
E-mail: info@zorgttp.nl

ZorgTTP
Privacy & vertrouwen

Document kenmerken

Titel	Methodebeschrijving TRES
Versie	1.0
Datum	9 februari 2024
Auteur	L. Baur, H. van Vlaanderen

Versiebeheer

Versie	Datum	Omschrijving	Auteur
0.9	2 februari 2024	Concept versie	L. Baur
1.0	9 februari 2024	Eerste publieke versie	L. Baur, H. van Vlaanderen

Inhoudsopgave

1. Terminologie

Decryptie
Het proces van ontsleuteling van (persoons)gegevens.

Data Management Applicatie (DMA):
Applicatie waarbinnen de te beveiligen onderzoeksgegevens zijn opgeslagen.

Dataregistratie
De verzameling van gegevens ten behoeve van één of meerdere gegevensverwerkingsdoeleinden.

Domein
Per registratiehouder wordt in TRES een domein ingericht.

Encryptie
Proces waarbij een leesbaar bericht wordt omgezet naar een versleuteld bericht.

Encrypted datablock
Resultaat van een bewerking op leesbare gegevens met behulp van een encryptiesleutel en een encryptiealgoritme. (zie API doc)

Gebruiker
De verzender van de te beveiligen gegevens. Tevens ontvanger van de door de dienstverlener beveiligde gegevens. Dit is altijd een persoon, gekoppeld aan een gebruikeraccount in TRES.

Project
Binnen een domein in TRES is elke gegevensverwerking ondergebracht in een eigen project. Dit betreft het geheel van afspraken, sleutelmateriaal en technische instellingen voor een bepaalde opdrachtgever.

Registratiehouder
De organisatie die de dataregistratie in beheer heeft. Doorgaans treedt de registratiehouder op als opdrachtgever richting de TTP.

TRES platform
Het geheel van ZorgTTP-applicaties, interfaces en technische voorzieningen dat in samenhang wordt ingezet voor het en- en decrypten van persoonsgegevens.

Trusted Third Party (TTP)
Door andere partijen vertrouwde organisatie. Specifiek voor pseudonimimisering blijkt het vertrouwen uit de opzet van en afspraken over de dienstverlening die zodanig is dat technische en organisatorische maatregelen het ongeautoriseerd doorbreken van de pseudonimisering voorkomen.

Verwerking
Een enkele versleuteling of ontsleuteling van een enkele waarde middels TRES.

2. Aanleiding

ZorgTTP is sinds 2007 actief als Trusted Third Party (TTP) en is gespecialiseerd in het ondersteunen van organisaties bij het op passende wijze beschermen van privacygevoelige informatie ten behoeve van beleids- en onderzoeksdoeleinden. ZorgTTP biedt zogenaamde Privacy Enhancing Technologies (PET) aan om gegevens te pseudonimiseren. Pseudonimisering kan daarbij zowel omkeerbaar als onomkeerbaar plaatsvinden. Om historische redenen zijn deze vormen van pseudonimiseren ondergebracht in aparte systemen. Na invoering van de Algemene Verordening Gegevensbescherming (AVG) is hiervoor feitelijk geen noodzaak meer. Het vormt wel de verklaring voor het feit dat voor onomkeerbare pseudonimsering reeds eerder een openbare methodebeschrijving is gepubliceerd. Deze dateert van voor de invoering van de AVG en houdt nadrukkelijk geen rekening met omkeerbare pseudonimisering. De use-case voor onomkeerbare pseudonimisatie is met name gericht op beleidsmakers en overheden omgevingen waar slechts met gepseudonimiseerde persoonsgegevens gewerkt mag worden, geen noodzaak bestaat om terug te kunnen naar de identificerende gegevens, maar wel behoefte bestaat om individuen op individueel niveau te kunnen onderscheiden en in tijd te kunnen volgen.

> *De uitwerking van de openbare onomkeerbare pseudonimisatiemethode is hier te vinden: https://www.zorgttp.nl/wp-content/uploads/2023/01/NEN-pseudonimisering-specificatie-voorstel-VWS-1.0.pdf*

In dit document vindt u de uitwerking van de door ZorgTTP gehanteerde methode voor omkeerbare pseudonimisering. Deze methode is ondergebracht in de TRES dienst. Daarbij staat TRES voor Trusted Reversible Encryption System. De TRES dienst is primair gericht op omkeerbare pseudonimisatie in het kader van wetenschappelijk onderzoek. TRES biedt privacybescherming binnen omgevingen waar met persoonsgegevens gewerkt mag worden. Deze vorm van pseudonimisatie is omkeerbaar, maar kan indien gewenst ook als onomkeerbare variant worden ingezet. Zowel de omkeerbare als onomkeerbare variant voldoen aan de definitie voor pseudonimisatie zoals opgenomen in de AVG.[1]

2.1 Doel van de beschrijving

Het doel van deze beschrijving is het bieden van transparantie met betrekking tot de opzet en werking van de TRES dienst. De beschrijving houdt rekening met de methodebeschrijving voor onomkeerbare pseudonimisering en de eisen die in de norm NEN 7524 worden gesteld. Omdat er momenteel geen certificeringsschema voorhanden is voor deze norm is in eigen beheer een verklaring van toepasselijkheid opgesteld met betrekking tot de in de norm opgenomen eisen.

2.2 Identificerende gegevens dienstverlener

De NEN7524 vereist het publiceren van identificerende gegevens door de dienstverlener. De identificerende gegevens van ZorgTTP zijn:

Adres: De Bouw 127, 3991 SZ in Houten
Telefoon: 030-63 606 49
E-mail: info@zorgttp.nl
BTW Nummer: NL807417269B01
KvK Utrecht: 30148110

[1] ZorgTTP verwijst in eigen documentatie vaak naar de omkeerbare TRES-dienstverlening als encryptiedienst, waar het naar de onomkeerbare variant verwijst als pseudonimisatiedienst.

Op de website van ZorgTTP zijn de actuele algemene leveringsvoorwaarden te vinden. Deze zijn gedeponeerd bij de Kamer van Koophandel.

2.3 Leeswijzer

In dit document volgt de methodebeschrijving van de omkeerbare pseudonimisatiedienst zoals dit is geïmplementeerd door ZorgTTP. Allereerst zijn in hoofdstuk 3 de eisen aan de pseudonimisatiedienst uiteengezet die het uitgangspunt vormen voor ZorgTTP. In hoofdstuk 4 volgt de vertaling daarvan naar de TRES encryptiedienst en het doel waaraan deze dienst invulling geeft. In hoofdstuk 5 is een concrete uitwerking opgenomen van TRES met informatie over de context, de opzet, het algoritme en de functionaliteiten. Concrete voorbeelden van gegevensverwerkingen en van een encrypted datablock zijn gegeven in de bijlagen.

3. Eisen aan de pseudonimisering

In onderstaande tabel zijn de uitgangspunten opgesteld van de cryptografische operaties en betrokken data structuren bij de aanbieder en bij de pseudonimiseringsdienst. Deze uitgangspunten zijn gebaseerd op de normen NEN 7524:2019, ISO 25237:2017 en de vereisten zoals opgenomen in de cryptografische specificatie onomkeerbaar pseudonimiseren die is opgesteld in opdracht van het Ministerie van Volksgezondheid, Welzijn en Sport (2015).

#	Uitgangspunt	Toelichting
1.	*Pseudoniemen zijn zowel omkeerbaar en onomkeerbaar*	NEN 7524, ISO 25237
2.	*Compartimentering van afnemer domeinen*	NEN 7524, ISO 25237
3.	*Authenticiteit van pseudoniemen beschermd*	De authenticiteit van de geëncrypteerde waarde moet kunnen worden vastgesteld door de pseudonimiseringsdienst. Dit is met name van belang als de pseudonimiseringsdienst domein conversie gaat uitvoeren ('translate', zie hoofdstuk 5.6.9), daarbij moet de pseudonimiseringsdienst zekerheid hebben dat hij (gevoelige) cryptografische operaties gaat uitvoeren op geëncrypteerde waarden die van *hemzelf* afkomstig zijn en niet op mogelijk gemanipuleerde data.
4.	*Cryptografische stand der techniek*	Dit wordt ook geëist in Artikel 25 van de Algemene Verordening Gegevensbescherming (AVG). Hiervoor hanteren wij [NIST] als basis.
5.	*Migreerbaarheid naar andere cryptografische sleutels*	Het moet mogelijk zijn om op een gegeven moment op andere cryptografische sleutels over te gaan, bijvoorbeeld omdat ze verouderd zijn of omdat er een beveiligingsincident is geweest bij de pseudonimiseringsdienst.
6.	*Migreerbaarheid naar andere algoritmen*	Het moet mogelijk zijn om op een gegeven moment op andere cryptografische algoritmen over te gaan, bijvoorbeeld omdat ze verouderd zijn en te weinig beveiliging bieden of omdat ze gebroken zijn.

7.	*Overdraagbaarheid ('portability')*	Het moet mogelijk zijn om op een gegeven moment de pseudonimiseringsdienst over te dragen aan een andere pseudonimiseringsdienst met minimale inspanning en impact voor de aanbieders en afnemers. Dit zou vorm gegeven kunnen worden doordat de huidige pseudonimiseringsdienst de betrokken cryptografische sleutels veilige overdraagt aan de nieuwe en dat de aanbieders en afnemers software van de nieuwe pseudonimiseringsdienst gaan gebruiken.
8.	*Compactheid* Pseudoniemen moeten zo min mogelijk data ('karakters) benutten.	Gepseudonimiseerde bestanden omvatten vaak grote populaties met dus vele pseudoniemen. Een langer pseudoniem betekent een groter bestand.
9.	*Representatie in printbare vorm*	Pseudoniemen moeten ook manueel kunnen worden bewerkt, e.g. in Excel. Om ongewenste neveneffecten te voorkomen, gaan we slechts uit van karakters die printbaar zijn.
10.	*(Eenvoudig) interpreteerbaar*	Pseudoniemen moeten ook handmatig kunnen worden verwerkt. Ook moet de pseudonimiseringsdienst in detail kunnen achterhalen welke sleutels en algoritmen zijn toegepast voor als er domeinconversie moet worden toegepast.
11.	*Koppelbaar*	Het moet mogelijk zijn om pseudoniemen voor dezelfde betrokkene binnen hetzelfde project steeds gelijk te laten zijn. Op die wijze kunnen gegevens in de tijd en over locaties heen op individueel niveau gekoppeld worden.

4. Het doel van TRES

TRES is een Privacy Enhancing Technology (PET). Met deze beveiligingsmaatregel wordt de identiteit van personen in een database geëncrypteerd (versleuteld) en daarmee onherkenbaar gemaakt. Dit is nuttig in dataregistraties waarbij behoefte is aan het registreren van identificerende gegevens, zoals bijv. voor het uitnodigen van deelnemers aan wetenschappelijk onderzoek of voor het traceren van orthopedische implantaten na plaatsing. In situaties als deze is het noodzakelijk om onder specifieke voorwaarden de identiteit van personen te kunnen vaststellen.

Met een combinatie van medische gegevens en identificerende gegevens beschikken deze *dataregistraties* over zeer privacygevoelige informatie. De opslag en verwerking van deze gegevens moet daarom met uiterste zorg plaatsvinden. Daarom wordt in opzet uitgegaan van de Privacy by Default en Privacy by Design principes.

Op basis van vooraf bepaalde autorisaties worden encryptie- of decryptierechten toegekend aan de medewerkers van een dataregistratie. Zij zijn *gebruikers* van de TRES dienst en kunnen waarden encrypteren en deze waarden decrypteren (ontsleutelen), mits zij beschikken over de juiste rechten. De rechten worden op basis van afspraken met de *registratiehouder* door de TTP beheerd. Het resultaat is dat de gegevens die "at rest" zijn steeds versleuteld zijn. Ontsleuteling kan enkel plaatsvinden middels TRES nadat en door daartoe bevoegde medewerkers binnen de dataregistratie. Alle versleutel- en ontsleutelingsacties worden gelogd binnen TRES. Daarmee kan aangetoond worden wie op welk moment welke gegevens heeft versleuteld of ontsleuteld.

De dienstverlening van ZorgTTP in het kader van TRES bestaat uit:

a. het beheer en de opslag van accountgegevens (authenticatie- en autorisatiegegevens) van gebruikers die encrypties en/of decrypties mogen uitvoeren
b. het beheer van de daar bijbehorende cryptografische sleutels en
c. het aanbieden van een online dienst die encryptie en decryptie mogelijk maakt.

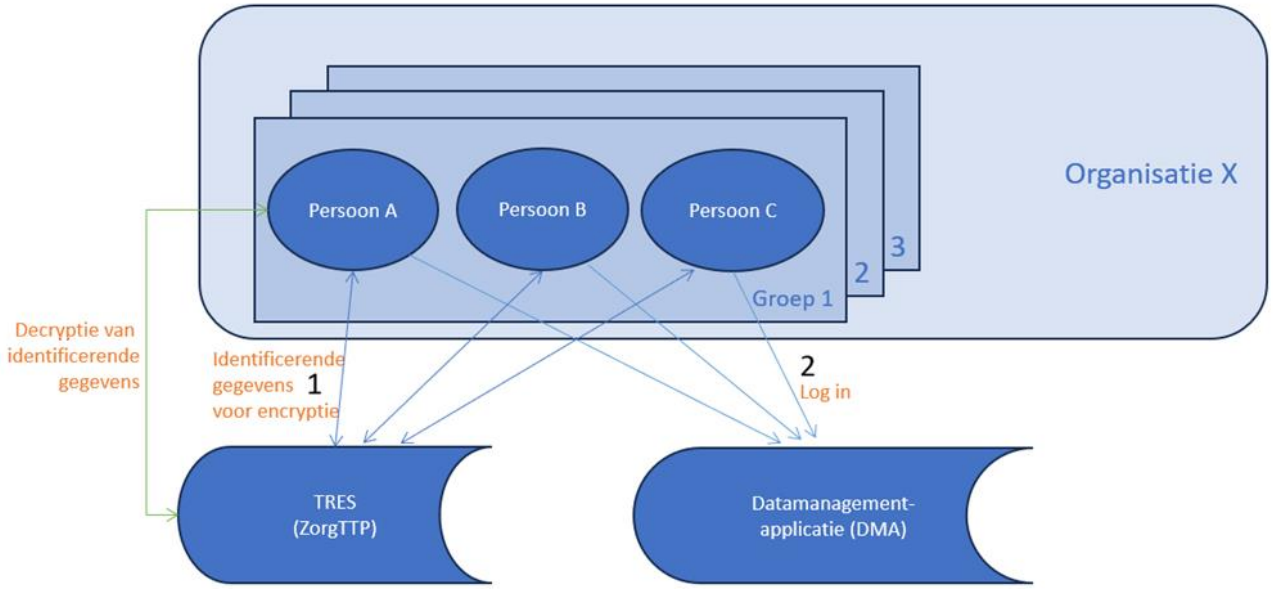
Uitgangspunt is dat TRES geen geëncrypteerde of ongeëncrypteerde waarden opslaat. TRES kent slechts de sleutels en rechten op die sleutels waarmee gegevens versleuteld zijn. De resultaatwaarden worden na verwerking door TRES teruggestuurd naar de gebruiker die de input heeft aangeboden. De gebruiker en daarmee de registratiehouder is uitdrukkelijk zelf verantwoordelijk voor de eventuele opslag van geëncrypteerde of ongeëncrypteerde waarden die het resultaat van een verwerking bij TRES zijn.

5. TRES applicatie

5.1 Context

TRES wordt in de meeste gevallen gebruikt in combinatie met een Data Management Systeem (DMA). Dit kan een eigen systeem zijn van de registratiehouder of een systeem van een derde leverancier. Het is ook mogelijk om TRES in te zetten in combinatie met de Privacy- en Verzendmodule (PVM), de pseudonimisatiesoftware van ZorgTTP. De combinatie van een DMA/PVM met TRES geeft een dubbele beveiliging. De DMA/PVM authentiseert de gebruiker voor toegang tot de data met de geëncrypteerde identiteit. Vervolgens volgt een onafhankelijke authenticatie bij TRES om de daadwerkelijke encryptie- of decryptiehandeling te mogen uitvoeren op basis van daartoe binnen TRES per gebruiker en project vastgelegde autorisaties.

Een voorbeeld van de TRES implementatie in combinatie met een DMA ziet er als volgt uit:

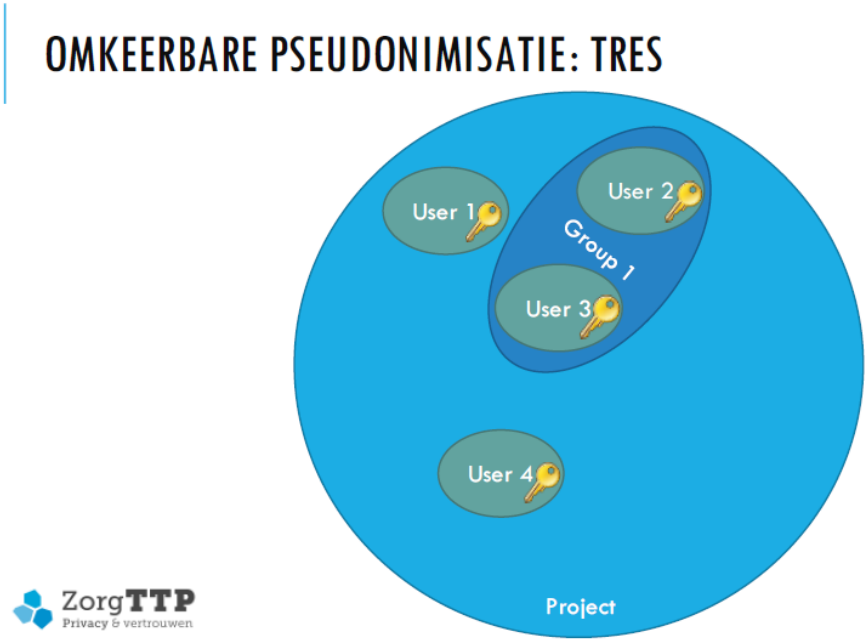


Afb. 1: De interactie tussen gebruikers van een organisatie met de DMA en TRES.

- In TRES is voor deze registratiehouder 'Organisatie X' één project ingericht met daarbinnen drie groepen (zie paragraaf 5.2 voor nadere toelichting op projecten en groepen);
- In groep 1 zijn drie gebruikersaccounts aangemaakt en actief;
- Het account ('persoon A') communiceert separaat met de TRES en de DMA, met als doel resp. encryptie van identificerende gegevens en inlog in de DMA.

5.2 Opzet: Domeinen, projecten en groepen

In de volgende plaat is zichtbaar op welke wijze de TRES encryptiedienst is opgezet.



Afb. 2: De opzet van TRES met groepen en gebruikersaccounts.

Per registratiehouder wordt in TRES een **domein** ingericht. Binnen dat domein is elke gegevensverwerking ondergebracht in een eigen **project**. **Gebruikers** behoren tot een specifiek project. Binnen het project kunnen gebruikers worden ondergebracht in **groepen**. Bijv. een groep voor datamanagers of een groep voor een specifieke zorginstelling.

TRES kent een groepsrecht systeem waarmee het recht tot decryptie van data gedeeld kan worden tussen gebruikers. Om rechten tussen gebruikers te delen wordt gebruik gemaakt van groepen binnen het project van de betreffende gegevensverwerking. Gebruikers kunnen als contributor hun data bijdragen aan een groep en gebruikers kunnen met decrypt recht toestemming krijgen om alle data die beschikbaar zijn in deze groep te mogen decrypteren. Deze rechten zijn asymmetrisch. Volgens hetzelfde groepsprincipe kan TRES ook gebruik maken van super/sub groepen. In dat geval overstijgen contribute en decrypt rechten tot meerdere groepen. Met dit rechten systeem kunnen de gangbare scenario's bij de DMA voor het delen van toegang worden ondersteund. Doordat de rechten door TRES worden bepaald bij elke encryptie en decryptie aanroep en het rechten zijn tussen gebruikers, zijn alle rechten-wijzigingen direct actief.

5.3 Interactie tussen de gebruiker en TRES

Het aanroepen van TRES vanuit een DMA/PVM wordt mogelijk gemaakt met de webservice functie in TRES. Hiervoor is een TRES API ontwikkelt waarmee externe systemen en applicaties toegang krijgen tot de encryptie- en decryptiefunctionaliteit van TRES. De verantwoordelijkheid voor het opzetten van de verbinding met TRES via de API ligt bij Opdrachtgever en zal in de praktijk worden gerealiseerd door de beheerder van de DMA.

5.4 Algoritme

De encryptie mogelijkheden binnen TRES zijn gebaseerd op twee methodes (van het .net framework) namelijk:

1. RijndaelEncryptionProvider.ToEncryptedBytes()
2. RijndaelSaltEncryptionProvider.ToEncryptedBytes()

Er wordt gebruik gemaakt van het Rijndael algoritme voor encryptie. Het Rijndael algoritme dat gebruikt wordt is hetzelfde algoritme als AES-256. Het verschil de methodes is dat methode 2 een salt gebruikt voor de encryptie en methode 1 niet.

De standaard waardes voor keysize, blocksize en ciphermode worden gehanteerd:

- Key size 256 bits
- Block size 128 bits
- Cipher mode CBC

De Key en IV (initialization vector) die voor de encryptie gebruikt worden zijn de Key en IV van de gebruiker. In TRES heeft elke gegevensverwerking een specifiek project binnen het eigen domein. Als de encryptie opdracht vanuit een project context wordt uitgevoerd – bijv. in geval van een search image (zie paragraaf 5.6.3) - dan wordt de Key en de IV van het betreffende project gebruikt.

TRES kent de mogelijkheid om onomkeerbare pseudoniemen te maken (zie paragraaf 5.6.4). Deze functie wordt 'translate to export' genoemd. Bijvoorbeeld voor data uitgifte in het kader van een onderzoek. Daarbij wordt de oorspronkelijke input eerst gehasht met HMAC SHA256 alvorens deze versleuteld wordt. Door de input te hashen en vervolgens te versleutelen is de oorspronkelijke input niet meer te achterhalen.

5.5 Functionaliteiten en rechten

TRES kent een aantal functies en rechten zoals hier nader is beschreven.

5.5.1 **Encryptie**

Tijdens het encryptieproces worden de volgende stappen doorlopen. Allereerst logt de gebruiker in bij zowel de DMA en TRES. De gebruiker wordt door beiden geauthentiseerd. De identificerende data elementen worden aangeboden aan de TTP voor encryptie mits de gebruiker daartoe geautoriseerd is binnen het project waarvoor de data wordt aangeboden. Dit gebeurt in de meeste gevallen via een webservice aanroep. TRES voert de encryptie uit en stuurt de gebruiker de resultaatwaarde. Deze geëncrypteerde waarde wordt daarna, in de meeste gevallen geautomatiseerd, ingevoerd in de DMA (Deze laatste stap valt buiten de scope van ZorgTTP en valt onder de verantwoordelijkheid van de registratiehouder. Het wordt hier echter genoemd om een volledig beeld te geven van de verwerkingsactiviteit). TRES maakt gebruik van persoonlijke encryptie. Voor een gebruiker is de encryptie van dezelfde waarde iedere keer gelijk. Dezelfde originele data zal voor verschillende gebruikers een verschillende encryptiewaarde opleveren.

5.5.2 **Decryptie**

In geval van een decryptie verlopen de stappen in omgekeerde richting. De gebruiker logt in in de DMA om toegang te krijgen tot medische gegevens met geëncrypteerde identificatie en krijgt daarbij

alleen toegang tot geautoriseerde informatie. Indien de gebruiker beschikt over decryptierechten, worden gedecrypteerde waarden uit de DMA applicatie vanuit de gebruiker aangeboden aan de TTP voor decryptie. Na authenticatie van de betreffende gebruiker door TRES wordt de identificerende (ongeëncrypteerde) waarde aangeboden aan de gebruiker.

5.5.3 **Zoeken in geëncrypteerde data met behulp van een search image**

Gezien TRES gebruik maakt van persoonlijke encryptie is het onmogelijk voor gebruikers om te zoeken in geëncrypteerde gegevens van andere gebruikers. Dit beschermt tegen het achterhalen van de identiteit van deelnemers. Om te achterhalen of meerdere gebruikers op verschillende records in de DMA data hebben ingevoerd voor dezelfde gebruiker kan gebruik worden gemaakt van het search image. Een search image is een extra geëncrypteerde waarde die automatisch wordt toegevoegd aan het encryptieresultaat. Een encryptieverzoek zal voor een zelfde originele waarde altijd dezelfde search image waarde geven. Dit is daardoor te gebruiken om op te zoeken of een specifieke waarde, bijv. patiënt-ID, voorkomt in de database. Deze search image is project specifiek. Het is daarmee alleen mogelijk binnen een project te zoeken en dit beschermd tegen ongewenst koppelen met ander projecten. Doordat het search image zeer sterk verschilt bij kleine wijzigingen in de originele waardes is het niet mogelijk met deelzoektermen of met wildcards te werken. Er kan alleen worden gezocht op een exacte match.

5.5.4 **Encryptie met extra random uitkomst (salt)**

Een encryptie van een specifieke waarde levert voor dezelfde gebruiker altijd dezelfde encryptiewaarde. In specifieke gevallen is het wenselijk om de geëncrypteerde waarde als resultaat van elke aanroep uniek te maken, bijv. in het geval van een beperkte keuzelijst zoals etniciteit.
De oplossing hiervoor is het toepassen van een salt; een extra random functie. Doordat de geëncrypteerde waarde bij iedere aanroep verschilt, zal ook de opgeslagen waarde in de DMA over alle records verschillend zijn. Een andere toegevoegde waarde van de salt is dat de toepassing ervan het zoeken op geëncrypteerde waarden onmogelijk maakt. Hiermee creëert het een extra beveiligingsmaatregel.

5.5.5 **On-behalf recht: encrypteren namens een andere gebruiker**

Het is mogelijk om de data door een centrale functionaris te laten invoeren namens bijv. één of meerdere andere gebruikers of zorginstellingen. TRES ondersteunt het beschikbaar maken van decryptie voor de bron (gebruiker of zorginstelling) met groepsrechten en met het on-behalf recht. Deze on-behalf optie is alleen van toepassing voor encryptie. Voor decryptie worden rechten enkel verleend op basis van de geauthentiseerde gebruiker en zijn groepsrechten.

De on-behalf functie werkt als volgt: Het eerste account is van de gebruiker die de invoer doet en daarmee inlogt, hier verder genoemd ‘invoerder’. Het tweede account is van de gebruiker voor wie die de data wordt geëncrypteerd en wordt hier het on-behalf account of gebruiker genoemd. Door gebruik van on-behalf zal de data worden geëncrypteerd met de gegevens van de onbehalf gebruiker. Het resultaat is daarmee hetzelfde als wanneer de on-behalf gebruiker de encryptie zelf zou hebben uitgevoerd. De geëncrypteerde data behoort daarmee dus toe aan de on-behalf gebruiker en zal ook via zijn groepen worden gedeeld met geautoriseerde gebruikers.

Encrypties kunnen ook worden gedaan namens een afdeling of groep middels anonieme on-behalf accounts per groep. Deze anonieme accounts kunnen ook gebruik worden voor bulk conversies per afdeling of groep.

5.5.6 **Server to server account**

Bij directe server koppelingen is er geen gebruikersinteractie. Dat maakt de reguliere password expire van accounts onwenselijk. Voor server koppelingen kan daarom gewerkt worden met server to server accounts. Deze accounts werken niet met een wachtwoord, maar met een wachtwoord-token wat niet zal verlopen. Als extra beveiliging zijn deze tokens een automatisch gegenereerde lange random waarde. Het token kan niet zelf gekozen worden en is altijd een complexe code.

5.5.7 **Communicatie met TRES vanuit een mobiele applicatie met automatische accounts**

Automatic accounts zijn gecreëerd voor projecten waarbij gebruik wordt gemaakt van TRES in combinatie met mobiele applicaties. Bij deze accounts zijn de user credentials gebaseerd op de user GUID en worden ze gegenereerd zonder tussenkomst van de gebruiker.

5.5.8 **Translate**

Deze instelling geeft het recht om channels te gebruiken. Accounts mogen geëncrypteerde gegevens opnieuw encrypteren met een andere sleutel. Dit maakt project- en domeinoverstijgende conversie binnen TRES mogelijk.

5.6 Verwerking en opslag van gegevens

TRES gebruikt sleutels om aangeboden data te encrypteren of decrypteren. Originele of geëncrypteerde data wordt niet permanent opgeslagen maar in-memory verwerkt. TRES encrypteert de identificerende gegevens en heeft daarmee tijdelijk toegang tot die informatie. De identificerende gegevens zijn gedurende enkele miliseconden tot maximaal enkele seconden aanwezig in het werkgeheugen op de server van TRES. Daarna worden de gegevens automatisch permanent verwijderd. Omdat de identificerende gegevens tijdelijk aanwezig zijn binnen de applicatie sluit ZorgTTP voor dit doel een verwerkersovereenkomst. Medewerkers van ZorgTTP hebben daarbij in de praktijk op geen enkele wijze directe toegang tot de servers waarop de TRES applicatie draait. Deze is slechts door daartoe geautoriseerde beheerders benaderbaar. De niet te versleutelen gegevens blijven binnen de DMA. Met deze werkwijze is sprake van een strikte functiescheiding tussen het versleutelen van en het werken met de versleutelde gegevens. ZorgTTP beschikt (tijdelijk) over identificerende gegevens, maar niet over medische informatie, en de DMA beschikt over de medische informatie, maar zonder identificerende gegevens.

5.7 Overdraagbaarheid (‘portability’)

ZorgTTP en haar opdrachtgevers hechten een groot belang aan het zorgvuldig omgaan met persoonsgegevens. De dienstverlening van ZorgTTP helpt om de gevoelige gegevens aantoonbaar en op passende wijze te beveiligen, zowel technisch als organisatorisch. In geval van een faillissement is ZorgTTP echter niet langer in staat om de dienstverlening aan te bieden. Registratiehouders worden in dit geval in de gelegenheid gesteld om de beveiliging van de gevoelige gegevens te continueren. De dienst zal in een dergelijke situatie tijdelijk bij de hosting partij worden gecontinueerd. De registratiehouder krijgt autorisatie om in die periode alle data van het project te ontsleutelen die via TRES is geëncrypteerd. Zij kunnen dit vervolgens bij een andere aanbieder opnieuw laten encrypteren. De overdracht van sleutelmateriaal is in dit geval niet noodzakelijk.

Bronnen

International Organization for Standardization (ISO). (2017). ISO 25237:2017, Health Informatics - Pseudonymization. Zie https://www.iso.org/standard/63553.html.

Ministerie van Volksgezondheid, Welzijn en Sport. (2015). Definitief voorstel voor cryptografische specificatie pseudonimisering. Zie https://www.zorgttp.nl/wp-content/uploads/2023/01/NEN-pseudonimisering-specificatie-voorstel-VWS-1.0.pdf.

National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS 140-2, November 26, 2001. Zie http://csrc.nist.gov.

National Institute of Standards and Technology (NIST), Recommendation for Key Management – Part 1: General (Revision 5), 800-57, mei 2020. Zie http://csrc.nist.gov.

National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS), FIPS 180-4, maart 2012. Zie http://csrc.nist.gov.

National Institute of Standards and Technology (NIST), The Keyed-Hash Message Authentication Code (HMAC), FIPS PUB 198-1, juli 2008. Zie http://csrc.nist.gov.

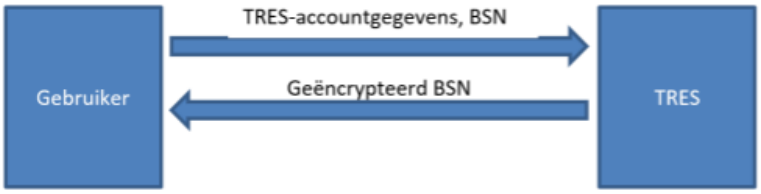
Nederlandse Norm (NEN). (2019). NEN 7524, Medische informatica – Pseudonimisatiedienstverlening. Verkrijgbaar via https://www.nen.nl/nen-7524-2019-en-259792.

The Internet Engineering Task Force, The Base16, Base32, and Base64 Data Encodings, RFC 4648, october 2006. Zie www.ietf.org.

Bijlage 1: Voorbeelden van gegevensverwerkingen met TRES

Voorbeeld 1

Een gebruiker wil een BSN encrypteren middels TRES. De gebruiker levert het BSN aan middels een aanroep bij TRES:



1. Het BSN komt aan bij TRES met een encryptieverzoek;
2. TRES bepaalt middels welk account gebruiker is ingelogd;
3. TRES bepaalt of de gebruiker mag encrypteren;
4. TRES bepaalt welke sleutel bij het gebruikersaccount van de gebruiker behoort;
5. TRES encrypteert het BSN;
6. TRES bepaalt tevens het search image indien dat gewenst is. Dit gebeurt middels het verkrijgen van een project specifieke sleutel en vervolgens het bepalen van een hash van het BSN, waarna de hash geëncrypteerd wordt middels de project specifieke sleutel;
7. Het totale encryptieresultaat wordt geretourneerd naar de gebruiker;

Het BSN is nu omgezet in het volgende encryptieresultaat, bestaande uit de velden zoals hierboven weergegeven:

<3><df6ee324f8c7><H4tQ18MnpOSR==><g5aESN9kOX7jOsfDno==><kRne76BMf+J09I1XFMMbMh85EIU=>

In dit encryptieresultaat is te zien dat de encryptie is uitgevoerd met de sleutel van gebruiker met unieke code df6ee324f8c7. Wanneer een andere gebruiker binnen hetzelfde project hetzelfde BSN zou hebben versleuteld, dan zou het encryptieresultaat er als volgt uit kunnen zien:

<3><a2ff62038bad><G2r016AlgOwT==><g5aESN9kOX7jOsfDno==><qFFe52gqvkpyuR4GTMH24TAarXP=>

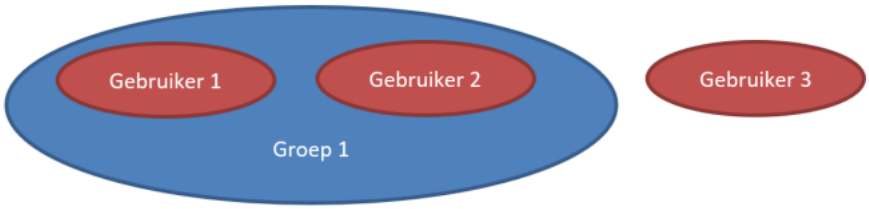
Dit encryptieresultaat laat zien dat het tot stand is gekomen middels een andere sleutel (a2ff62038bad), waardoor de versleutelde waarde anders is. Echter, de onderstreepte waarde (het search image) is hetzelfde, omdat hetzelfde BSN versleuteld is door twee gebruikers die in hetzelfde project zitten.

Bij decryptie dient de gebruiker de waarde opnieuw aan te bieden aan TRES bij het aanroepen van de decryptiefunctie:

1. De volledige geëncrypteerde string, zoals hierboven weergegeven, komt aan bij TRES met een decryptieverzoek;
2. TRES bepaalt middels welk account gebruiker is ingelogd;
3. TRES bepaalt of het encryptieresultaat niet corrupt is door de signature van het encryptieresultaat te valideren. Indien het encryptieresultaat corrupt is, zal er een foutmelding geretourneerd worden naar de gebruiker en is decryptie niet mogelijk;
4. TRES bepaalt of de gebruiker mag decrypteren op basis van de gespecificeerde sleutel in het encryptieresultaat;
5. TRES zoekt de sleutel op waarna gerefereerd wordt in het encryptieresultaat;
6. TRES decrypteert de geëncrypteerde string;
7. Het gedecrypteerde BSN wordt geretourneerd naar gebruiker.

Voorbeeld 2

In dit voorbeeld zijn er meerdere gebruikers betrokken met ieder verschillende rechten. Hierbij wordt gebruikgemaakt van de eerder genoemde groepenfunctionaliteit.



Gebruiker	GUID	Encryptierechten in groep 1	Decryptierechten in groep 1
Gebruiker 1	df6ee324f8c7	Ja	Ja
Gebruiker 2	a2ff62038bad	Ja	Ja
Gebruiker 3	d3f44501329a	Nee	Nee

Gebruikers 1 en 2 zitten in één groep en zouden bijvoorbeeld in de praktijk onderdeel uit kunnen maken van één maatschap binnen een ziekenhuis, waarbij beide gebruikers elkaars data mogen zien en dus decryptierechten hebben voor elkaars data. Gebruiker 3 maakt geen onderdeel uit van die groep en mag geëncrypteerde waarden van gebruikers 1 en 2 niet decrypteren. Andersom kunnen gebruikers 1 en 2 ook geen geëncrypteerde waarden van gebruiker 3 decrypteren.

Wanneer gebruiker 1 een BSN wil encrypteren, gebeurt dat zoals benoemd bij voorbeeld 1 en kan dat bijvoorbeeld het volgende encryptieresultaat opleveren:

<3><df6ee324f8c7><K9tR19MnpOTN==><u7aESN9kOX7jOsfDpr==><pNte96BHf+J09I1XFMMbMh85=>

In dit encryptieresultaat is te zien dat de encryptie door gebruiker 1 is uitgevoerd, daar de GUID df6ee324f8c7 overeenkomt met die van gebruiker 1.

Gebruiker 1 kan dit encryptieresultaat ergens opslaan waar overige gebruikers ook toegang toe hebben (in de DMA). Wanneer gebruiker 2 deze geëncrypteerde waarde probeert te decrypteren, zal TRES detecteren dat de waarde geëncrypteerd is met een sleutel van gebruiker 1 en dat gebruiker 2 bij gebruiker 1 in groep 1 zit. Tevens zal TRES zien dat gebruiker 2 decryptierechten heeft in die groep en dat gebruiker 2 dus gerechtigd is om de waarde te decrypteren. Wanneer gebruiker 3 dit zou proberen, zal dat niet lukken, daar gebruiker 3 niet in dezelfde groep zit als gebruiker 1 en dus geen decryptierechten heeft voor dit encryptieresultaat.

Bijlage 2: Opbouw van het encrypted datablock

Het encrypted datablock bestaat uit een aantal velden in vaste volgorde, gescheiden door dubbele punten (::).

Naam	Type	Lengte	Omschrijving
Protocolversie	Integer	1	Deze heeft altijd de waarde 3. Toekomstige releases van TRES kunnen mogelijk met een andere waarde werken. De gebruiker mag aannemen dat de opbouw van een encryptieresultaat hetzelfde is voor een gelijk protocolversienummer.
User GUID	GUID	36	De TRES-interne identificatie van de gebruiker. Voorbeeld: 3F2504E0-4F89-11D3-9A0C-0305E82C3301, zie http://nl.wikipedia.org/wiki/Globally_Unique_Identifier.
Encrypted value	Base64[2]	Variabel	Bevat de wijze van versleuteling en de versleutelde plaintextstring: • Prefix "1:" geeft aan dat de waarde versleuteld is zonder salt. • Prefix "2:" geeft aan dat de waarde versleuteld is met een random salt. De lengte van dit veld hangt af van de lengte van de plaintextstring (text) en de setting van de salted encryption (se).
Search Image	Base64	64	Deze heeft altijd de prefix "1:" Wanneer er geen search image aangevraagd is, staat er alleen een "::".
Signature	Base64	44	Een hash code over alle velden van het encryptieresultaat (responsemessage). Achtergrondinformatie: de signature is een SHA-256 met een project specifieke salt. In alle gevallen kan hiermee door ZorgTTP de integriteit van de velden worden aangetoond alvorens een decryptie plaatsvindt.

[2] Het komt in de praktijk soms voor dat '+'-tekens in het encrypted datablock 'wegvallen'en vervangen worden door spaties. Controleer bij een decryptieverzoek dat er geen spaties in het encrypted datablock aanwezig zijn; en vervang deze zo nodig weer door een "+"-teken.

De lengte van het encrypted datablock

Situatie 1: geen salted encryptie, geen search image:

Lengte plaintextstring	Lengte encrypted datablock
1 … 15	115
16 … 31	135
32 … 47	155
48 … 48 + 16n	155 + 20n

Situatie 2: geen salted encryptie, wel search image

Lengte plaintextstring	Lengte encrypted datablock
1 … 15	181
16 … 31	201
32 …63	221
48 … 48 + 16n	221 + 20n

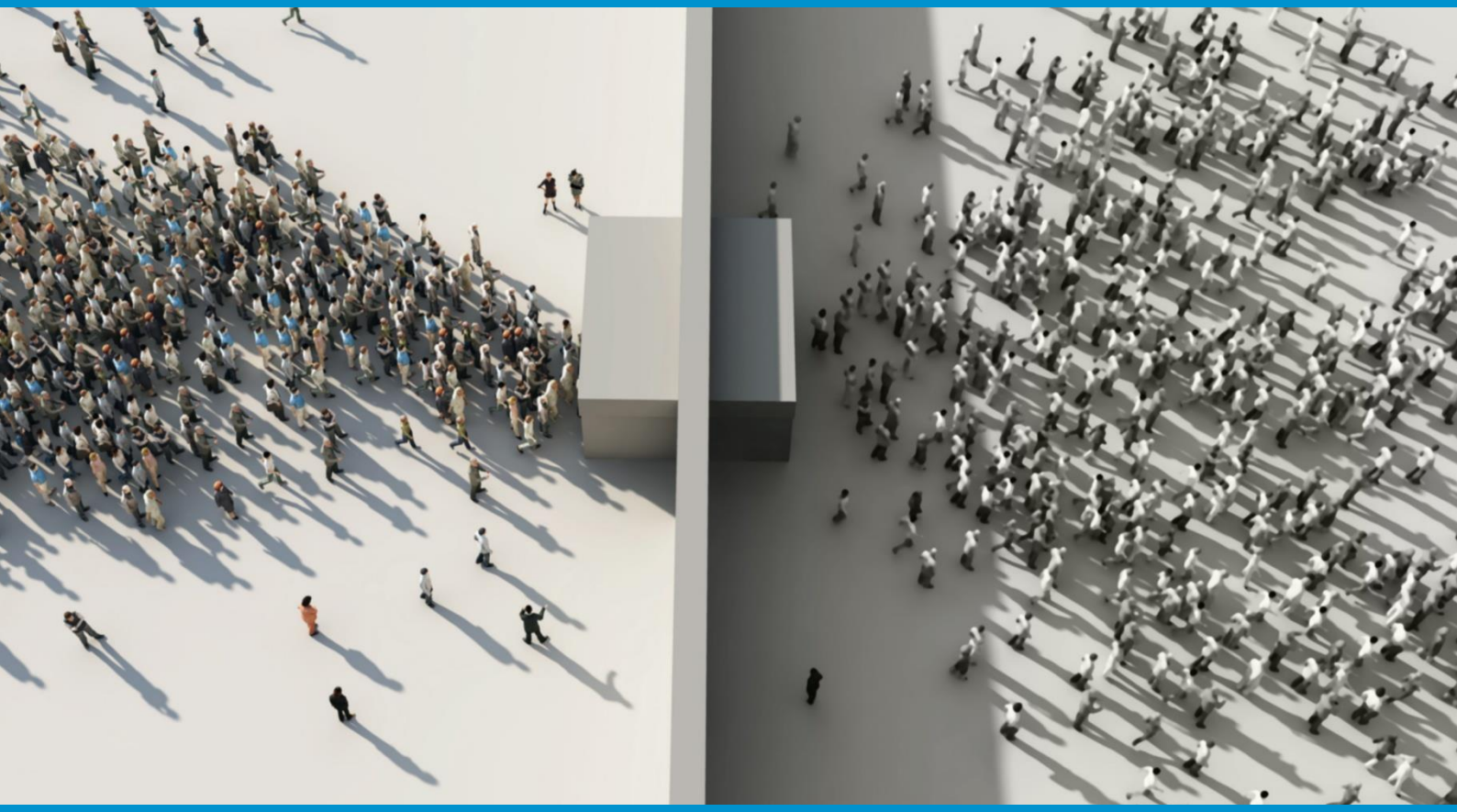
Situatie 3: wel salted encryptie, geen search image

Lengte plaintextstring	Lengte encrypted datablock
1 … 11	135
12 … 27	155
28 …etc.	175
28 … 28 + 16n	175 + 20n

Situatie 4: wel salted encryptie, wel search image

Deze situatie komt niet voor.

ZorgTTP
Data veilig delen



Methodebeschrijving TRES

9 februari 2024

L. Baur, H. van Vlaanderen

ZorgTTP
De Bouw 127
3991 SZ Houten
Telefoon: 030 – 63 606 49
E-mail: info@zorgttp.nl