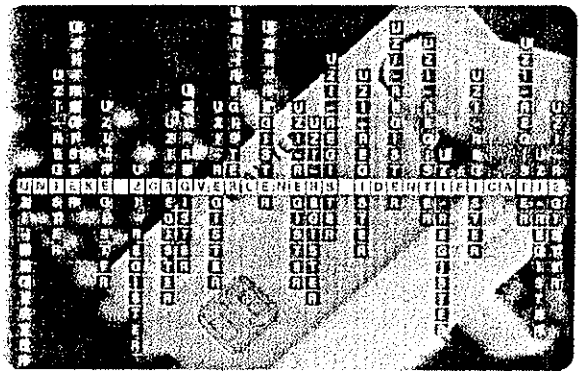

0101UZI0100REGISTER10111

Aanbevelingen beveiliging werkplek pashouder

Elektronische communicatie speelt een steeds grotere rol in onze samenleving. Ook in de zorg.
Omdat zorginformatie over het algemeen privacy gevoelige gegevens bevat, staat zorgvuldige bescherming van die gegevens voorop.
De patiënt moet daarop kunnen vertrouwen.
Het moet duidelijk zijn wie gegevens leest, verstuurt of ontvangt. Om hierover zekerheid te kunnen geven is het Unieke Zorgverlener Identificatie register, kortweg UZI-register, ontwikkeld.
Het UZI-register is onderdeel van het CIBG, agentschap van het ministerie van Volksgezondheid, Welzijn en Sport (VWS).
Het UZI-register maakt ook deel uit van het Informatiepunt BSN in de zorg en landelijk EPD.

Dit is een factsheet van het UZI-register, waarin een vaak gestelde vraag wordt beantwoord.
Een overzicht van alle factsheets vindt u op onze website www.uzi-register.nl.

April 2008

Om op de UZI-pas te kunnen vertrouwen is het belangrijk dat deze in een veilige werkomgeving gebruikt wordt. Deze factsheet is bedoeld om organisaties en medewerkers in de zorg te helpen om de werkomgevingen, waar UZI-passen worden gebruikt, veilig te maken.

Waar vindt u de juiste informatie?

- De NEN7510: Norm voor Informatiebeveiliging in de zorg en de NEN7512: Vertrouwensbasis voor gegevensuitwisseling (www.nen7510.org).
- De eisen PKI Overheid en ETSI TS 101456 norm: verplichtingen voor certificatie autoriteiten voor het uitgeven van gekwalificeerde certificaten (www.pkioverheid.nl).

Deze normenkaders zijn een belangrijke richtlijn. We lichten ze hieronder kort voor u toe.

NEN7510

Voor de inrichting van een veilige omgeving zijn algemene beveiligingseisen belangrijk zoals in de norm voor informatiebeveiliging in de zorg.
Deze norm geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die een pashouder dient te treffen ter beveiliging van de informatievoorziening.

NEN7512

De NEN7512 'Vertrouwensbasis voor gegevensuitwisseling' vormt een verdieping en uitbreiding van NEN7510. In de eerste plaats specificeert het niveaus voor het vertrouwen dat in de communicatiepartner moet worden gesteld bij het uitwisselen van gegevens in de zorg. In de tweede plaats levert het de aanzet tot risicoclassificatie en de uitwerking van de eisen uit NEN7510 ten aanzien van identificatie en authenticatie.

Eisen PKI Overheid en ETSI TS 101456 norm

De dienstverlening van het UZI-register is gecertificeerd op basis van ETSI TS 101 456 en voldoet daarmee aan de eisen zoals gesteld aan certificatiedienstverleners in de Wet elektronische handtekening. Het UZI-register voldoet ook aan het normenkader van de PKI voor de overheid zoals gesteld in het Programma van Eisen (zie www.pkioverheid.nl; PKI eisen).
Het UZI-register is bij de OPTA geregistreerd als getoetste uitgever van gekwalificeerde certificaten aan het publiek.

In het handboek PKI voor proceseigenaren, te vinden op www.pkioverheid.nl is het proces beschreven om een Public Key Infrastructure (PKI) te implementeren in een organisatie. Daarnaast is van belang dat bij de ontwikkeling van applicaties waarin zorgaanbieders en indicatieorganen gebruik maken van een UZI-pas de juiste waarborgen worden getroffen. Richtlijnen voor applicatieontwikkeling zijn te vinden in het programma van eisen van PKI overheid onder PKI-eisen -> programma van eisen.

En wat kunt u nog meer doen?

Naast de algemene waarborgen kunnen diverse UZI-pas specifieke beveiligingsmaatregelen worden getroffen. Aan de achterkant van deze factsheet vindt u de belangrijkste risico's en mogelijke maatregelen.

PIN-code in verkeerde handen
Als de PIN- of PUK-code in verkeerde handen valt, is het belangrijkste beveiligingsmechanisme voor misbruik van de pas verloren. Iemand die de PIN- of PUK-code weet en de pas in handen krijgt, kan deze onrechtmatig gebruiken.
Bijvoorbeeld in de volgende situaties:
- PIN-mailer niet achter slot en grendel opgeborgen.
- PIN- of PUK-code is voor anderen leesbaar opgeschreven.
- Anderen kijken mee bij invoering PIN-code.
- Loggen toetsenbordaanslagen door anderen.

Mogelijke maatregelen zijn:
- Pashouder bewust maken van de risico's.
- PIN-mailer in kluis, PIN-code uit het hoofd leren.
- Nooit de PIN- en PUK-code opschrijven en nooit de UZI-pas uitlenen.
- Het plaatsen van een apart numeriek toetsenbord dat kan worden afgeschermd bij invoeren PIN-code.
- Het gebruik van een kaartlezer waarop de PIN-code op de kaartlezer zelf wordt ingevoerd. Hiermee voorkom je het achterhalen van PIN-codes via logging van toetsenbordaanslagen.
- Visuele controle op hardwarematige loggers van toetsenbordaanslagen.
- Controle op spyware, virussen e.d.
- Fysiek afschermen van het gebruikte systeem.
- Wijzigen van de PIN-code als men vermoedt dat anderen deze kennen.

Onzorgvuldig gebruik UZI-pas
De houder van een UZI-pas moet de pas beschermen tegen beschadiging, verlies of diefstal, de pas niet onbewaakt achter laten en deze niet uitlenen. Anders kunnen onbevoegden de beschikking krijgen over de pas en misbruik maken van de pas door toegang te zoeken tot gegevens of een elektronische handtekening te zetten.

Mogelijke maatregelen zijn:
- Voorlichting over hoe met de pas om te gaan.
- Toezicht door beveiligingsfunctionaris of collegiale controle.
- Registratie en rapportage beveiligingsincidenten.
- Redenen voor uitlenen voorkomen.
- Afspraken opnemen in arbeidscontract of separate overeenkomst.

Meer informatie?
Indien u meer informatie wenst, kunt u terecht op de website van het UZI-register: www.uzi-register.nl, een e-mail sturen naar info@uzi-register.nl of bellen met telefoon 070-3406020.

Onterecht gebruik bestaande sessie
Als de sessie na het verwijderen van de UZI-pas niet wordt afgesloten kunnen onbevoegden de sessie misbruiken.

Mogelijke maatregelen zijn:
- Voorlichting geven over de applicaties waarin de UZI-pas wordt gebruikt.
- Afsluiten van de browser door de pashouder bij verlaten van de werkplek.
- Beveiligen van de toegang tot de pc met een schermbeveiliging met wachtwoord bij het verlaten van de werkplek.
- Applicatie geforceerd laten afsluiten van een sessie na een periode van non-activiteit bij de realisatie van applicaties.

Onbewust elektronisch ondertekenen documenten
De wetgeving over de elektronische handtekening stelt dat het voor de gebruiker duidelijk moet zijn dat deze een document geldig ondertekent, de inhoud begrijpt en onderschrijft.

Mogelijke maatregelen zijn:
- Voorlichting geven over de betekenis en het gebruik van de functies elektronische handtekening en authenticatie op de UZI-pas.
- Het bewust zetten van een elektronische handtekening afdwingen doordat de applicatie bij elk te tekenen document vraagt om de PIN-code in te voeren bij het zetten van de handtekening.

Private sleutel van servercertificaat in verkeerde handen
De sleutelparen die op een UZI-pas worden uitgegeven, worden door het UZI-register gegeneerd in een streng beveiligde omgeving. Een uitzondering hierop is het sleutelpaar dat hoort bij een servercertificaat. Dit wordt gegenereerd buiten het UZI-register. In de meeste gevallen zal dat op een systeem van een zorgaanbieder of indicatieorgaan zijn. Hierdoor ontstaat het risico dat de private sleutel onvoldoende wordt beschermd tegen kopiëren, wijzigen, verwijderen of ongeautoriseerd gebruik.

Maatregelen zijn:
- De private sleutel die hoort bij een server-certificaat alleen genereren en plaatsen in een fysiek afgesloten ruimte zoals een computerruimte of afsluitbare serverkast.
- Gebruik maken van een veilig middel voor opslag als een HSM (Hardware Security Module) voor het genereren van het sleutelpaar en de bevelliging van de private sleutel die bij het servercertificaat hoort.