

Verbetering governance TLS

Dirk Linden

Werkgroep Informatiebeveiliging en Privacy

11 april 2019, Architectuurraad

Situatie

Korte inventarisatie (niet uitputtend) van standaarden en voorzieningen bij Kennisnet met eigen uitspraken over beveiliging op niveau van transport en gegevens

- **UWLR:** Verwijs naar Certificeringsschema
- **Nummervoorziening:** TLS versie, verwijzing naar NCSC
- **ECK D&T:** poort, certificaat; verwijzing naar Certificeringsschema
- **Normenkader certificeringsschema:** TLS versie, IPSEC, AES versie; verwijzing naar NCSC
- **Edukoppeling transactiestandaard:** Verwijzing naar Digikoppeling
- **OSO/beveiliging:** Certificaten en validaties, protocollen, poort, TLS versie, eigen lijst ciphersuites, validatie op gedrag client en server
- **Digikoppeling:** TLS versie, poort, neemt selectie ciphersuites over van NCSC

Voorstel voor governance

- Beleg beheer van relevante standaarden voor versleuteling en ondertekening van gegevens en gegevenstransport op een centrale werkgroep (bijv (sub) werkgroep IBP)
- Vraag betrokken partijen om expertise en input voor deze werkgroep bij te dragen
- Draag de werkgroep op om standaarden te coördineren met rijksbrede werkgroepen
- Draag de werkgroep op om regelmatig en ad-hoc de relevante standaarden bij te werken

... en zie er dan op toe dat alle standaarden en voorzieningen in het onderwijs hierop aansluiten...