Memo: Waarom vereisen we Poort 443 voor Digikoppeling

Datum: 08-09-2016 | Door: Martin van der Plas | Doelgroep: Technisch Overleg Digikoppeling

In de Digikoppeling standaard wordt verwezen naar het verplicht gebruik van TLS*. In de standaard is dit specifieke aspect beschreven in het document "Digikoppeling beveiligingsstandaarden en voorschriften". Uitgaande van eis TLS005 wordt ons voorgeschreven dat : Voor communicatie over HTTPS wordt port 443 gebruikt. In onderbouwing wordt gesteld dat we TLS doen in verband met de beveiliging en authenticatie van organisaties met behulp van PKIOverheid. Het document specificeert namelijk niet waarom nu juist poort 443 wordt vereist...
...en aangezien TLS technisch ook werkt op andere poorten en daarmee dezelfde doelen worden bereikt is terecht de vraag belegd: "Waarom vereisen we Poort 443 voor Digikoppeling?"

Een deel van het antwoord is al te vinden op dezelfde pagina waar deze eis staat, de inleiding verwijst namelijk al naar IETF RFC 2818**.

Deze standaard beschrijft in basis de opzet van TLS over HTTP (ofwel HTTPS) en stelt in paragraaf 2.3 dat poortnummer 443 dient te worden gebruikt. Vrij vertaald stelt het echter vooral dat er voor andere initiële data wordt verwacht bij http dan bij https en er daarom een andere poort nodig is dan de standaard poort van http (poort 80). ook stelt het dat wanneer HTTP/TLS over TCP/IP wordt gebruikt de standaard poort 443 is.

Het geeft echter geen uitsluitsel waarom de standaardpoort 443 is en waarom een standaard nodig is.
Wikipedia*** heeft een overzicht van alle poortnummers en typeert ook of het een officiële poort is onder beheer van IANA (Internet Assigned Numbers Authority) een onderdeel van ICANN****

ICANN heeft als doel het internet veilig stabiel en interoperabel te houden. Dit is in lijn met het vasthouden aan 1 standaard poort voor HTTPS. Je weet dan namelijk altijd dat verkeer over poort 443 veilig is omdat het TLS afdwingt. Als je nooit een andere poort dan 443 gebruikt weet je dat het stabiel is en blijft en systemen zijn interoperabel omdat ze er vanuit kunnen gaan dat als men luistert naar poort 443 er alleen TLS verkeer hoeft te worden afgehandeld en met voor TLS verkeer nooit een andere poort hoeft open te stellen.

De reden dat we poort 443 gebruiken is gebaseerd op historie. Dit is namelijk nog steeds de oorspronkelijke poort die Kipp E.B. Hickman, een ontwikkelaar van Netscape, in 1994 heeft gekozen bij de ontwikkeling van SSL, de voorloper van TLS. Het gebruik van deze poort is vastgelegd in IETF RFC 1700***** Een samenvatting van deze historie is beschreven

op: http://www.howtogeek.com/233383/why-was-80-chosen-as-the-default-http-port-and-443-as-the-default-https-port/

Tot slot:
Wanneer je afwijkt van Poort 443 dient de gebruiker van de site of de service naast https ook het afwijkende poortnummer in de URI te specificeren. Het is sterk aanbevolen voor publieke services en sites om poort 443 te handhaven en met behulp van een firewall rule of proxy pass het verkeer intern te redirecten naar een afwijkende poort. Het verbergen van een open poort door een afwijkend poortnummer te gebruiken heeft geen zin omdat port scans eenvoudig open en toegankelijke poorten ontdekken.

*
zie https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/aansluitdocumentatie/Digikoppeling_Beveiligingsstandaarden_en_voorschriften_v1.pdf pagina 12 HS 4
** zie ook https://tools.ietf.org/html/rfc2818
*** https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
**** https://www.icann.org/
*****https://tools.ietf.org/html/rfc1700