Van	PinkRoccade Local Government
Aan	Klant Makelaarsuite / Berichtenmodule
Datum	2 februari 2016
Classificatie	Vertrouwelijk

Technische toelichting aanpassen 1024 bits certificaten Makelaarsuite

Inhoud

1 Wijze van controle type huidige certificaat 2

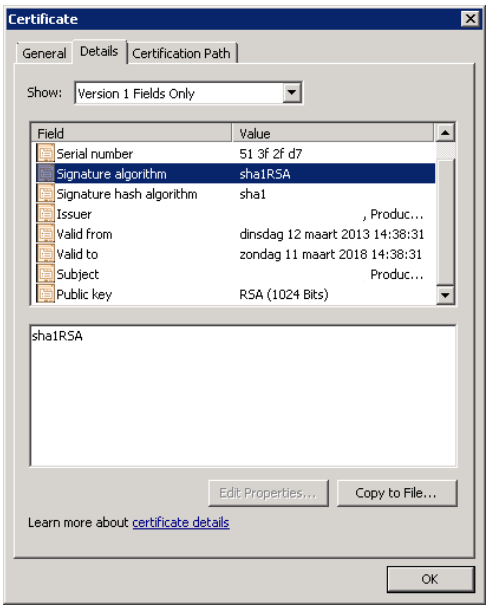
2 Technische toelichting 3

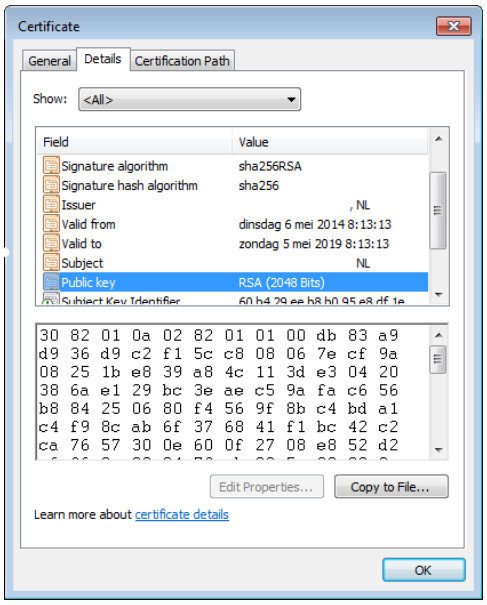
1 Wijze van controle type huidige certificaat

Indien uw Makelaarsuite / Berichtenmodule recent in gebruik is genomen is de kans groot dat u reeds over een correct certificaat beschikt. Op onderstaande wijze kunt het huidige certificaat controleren:

- Open in de browser de Makelaarsuite URL
- Klik vervolgens op een van onderstaande icoontjes

- Kies vervolgens voor ‘View certificate details’ of ‘Meer informatie’.
- En klik op het tabblad ‘Details’.





In bovenstaande afbeeldingen zijn voorbeelden zowel een veilig en een onveilig certificaat te zien.

- Veilig = 2048 bits en SHA-256
- Onveilig = 1024 bits en SHA-1

Deze onveilige certificaten moeten vervangen worden.

2 Technische toelichting

De beveiligde communicatie tussen twee webservices heeft een vaste routine van vaststellen van de identiteit en vervolgens het versleutelen van vervolgcommunicatie.
De communicatie begint initieel met een 'handshake'; op beide webservices is een privaat deel van een certificaat aanwezig en het publieke deel is aan de te koppelen webservice uitgereikt.

De webservices bepalen of de webservice aan de andere zijde te vertrouwen is, dit gebeurt op basis van het aantal bits in het certificaat.
Als de webservices elkaar vertrouwen is er een 'trust', de vervolgcommunicatie wordt gedaan op basis van de cryptografische mogelijkheden van het certificaat (SHA-1 of SHA-256 in het geval van de Makelaarsuite) en wordt een cryptografisch protocol (TLS of SSL) vastgesteld om de communicatie verder mee in te richten.

Binnen het cryptografisch protocol (TLS of SSL) bepaalt vervolgens het aantal 'Ciphers' de uiteindelijke versie van het protocol tijdens de 'negation phase', de onderhandeling over het 'shared secret', bijvoorbeeld TLS 1.1, 1.2, SSL 3.0 of 2.0.
De 'Ciphers' staan voor een cryptografisch algoritme (SHA betekend Secure Hashed Algorithm) en een vastgestelde sterkte in bits (in geval van de Makelaarsuite 1024-bits of 2048-bits).

Als resultaat van de onderhandeling wordt er een 'shared secret' vastgesteld dat alleen tussen de twee webservices bekend is. Dit omdat het steeds opnieuw volledig versleutelen en ontsleutelen van berichten aan de hand van het certificaat teveel rekenkracht en tijd kost en om een efficiënte communicatie te garanderen wordt voor de geëncrypte verbinding gebruik gemaakt van dit 'shared secret'.
De webservice met de hogere cryptografische mogelijkheden zal zich aanpassen naar de webservice met minder hoge cryptografische mogelijkheden.

Meer informatie over het niet langer ondersteunen van het SHA-1 algoritme door browsers is te vinden in twee artikelen op Security.nl:
https://www.security.nl/posting/441903/Google%2C+Microsoft+en+Mozilla+stoppen+RC4-support+in+2016

https://www.security.nl/posting/450026/Microsoft+overweegt+SHA-1-certificaten+eerder+te+blokkeren

Meer informatie over SHA en de beveiligde communicatie tussen webservices via onderstaande linkjes:
https://nl.wikipedia.org/wiki/SHA-familie

https://nl.wikipedia.org/wiki/Transport_Layer_Security de Engelstalige versie is completer en complexer:
https://en.wikipedia.org/wiki/Transport_Layer_Security

Ook 'De Correspondent' heeft een mooi stuk hierover geschreven dat gratis beschikbaar is:
https://decorrespondent.nl/691/Hoe-werkt-encryptie-op-internet-/52838769555-c6c0f16c