Verslag over de 1.7-XAdES beslissingen genomen in de VISI Expertcommissie van woensdag 29 november 2023.
Aanwezig hierbij waren Niek Pluijmert, Stefan Brouwers, Jos Hamilton, Tessa de Roos, Fiodor Bodnar, Jeroen Hiemstra en Arne Bruinse.

Inleiding

Bij de implementatie van XAdES in VISI zijn we erachter gekomen dat het zeer complex tot onmogelijk is om een private key /certificaat van een eIDAS trusted service op een server van een VISI leverancier te krijgen. Dit lijkt te komen doordat zo'n certificaat aan zulke hoge veiligheids eisen moet voldoen, dat deze alleen op externe handmatig te bedienen apparaatjes mag staan, of op de (externe) server van de (EU/eIDAS geaccrediteerde)certificaat leverancier. Dit geldt ook voor de "Time stamp server" om aan een cryptografisch ondertekend tijdstip te komen, zodat ook het tijdstip van ondertekenen 100% waterdicht is vastgelegd.

Aangezien XAdES in beginsel geen eis was in de oorspronkelijke probleemstelling aan de VISI Expertcommissie, hebben we getoetst of een afwijking van deze certificaat eis nog steeds de oorspronkelijke vraagstelling afdekt. XAdES was vooral een keuze van de VISI Expertcommisie om een zo duidelijk en uitgebreid mogelijke (open) standaard van ondertekenen te gebruiken. Dit vooral omdat de eerdere poging in VISI versie 1.5 strandde op details hoe een ondertekening precies moet werken. Daarnaast levert XAdES de mogelijkheid om een 100% juridisch geldige digitale handtekening aan een bericht mee te geven.

Uit onze toets hebben wij geconcludeerd dat de hieronder uitgewerkte afwijking nog steeds ruimschoots de oorspronkelijke vraag afdekt. Verder is de afwijking zo vormgegeven, dat het gebruik van 100% XAdES (met eIDAS certificaat) ook mogelijk blijft, naast de minder scherpe optie.
Dus als een VISI klant de software leverancier in de toekomst vraagt om een koppeling met hun private key server/device oid, dan is de VISI systematiek hierop voorbereid en zal de ondertekende berichten kunnen valideren via de eIDAS **P**ublic **K**ey **I**nfrastructure van de Europese unie. Op dit moment is deze vraag nog bij geen van de software leveranciers en de Expertcommissie bekend.

De oorspronkelijke eisen die de Expertcommissie mee kreeg, waren er allemaal op gebaseerd dat met 100% zekerheid te herleiden is dat een VISI bericht niet aangepast is na verzending door de verzender. Voor VISI 1.7 regelen we dat nu met deze uitbreiding. In een latere VISI versie zal dit bijvoorbeeld ook nog in VISI archieven doorgevoerd moeten worden.

Ter informatie - Technische uitleg van het ondertekeningsmechanisme:

In de cryptografie wordt gesproken over een "keypair": de "private key" en de "public key". Hiermee kan de private key iets versleutelen en alleen de bijbehorende public key dit ontsleutelen.

Zodra een VISI XML bericht verzonden wordt, wordt er een "hash" van dat bericht uitgerekend. Dit is een reeks karakters die iedereen op basis van dat specifieke bericht op dezelfde manier kan uitrekenen. Met die hash waarde wordt vervolgens samen met de private key een ondertekeningswaarde uitgerekend. Dit is een versleuteling van die hash waarde.
De public key van de verzender moet openbaar beschikbaar zijn. In het geval van XAdES officieel dus via de eIDAS PKI. In VISI 1.7 komt er een laagdrempelige oplossing naast. Vervolgens kan de ontvangende partij de hash van het bericht opnieuw uitrekenen en die valideren aan de public key van de verzender. Want alleen met de private key kun de ondertekening uitrekenen. Alleen met de public key, die bij die private key hoort, kan de ondertekening ontsleuteld worden. Als de ontsleutelde waarde gelijk is aan de uitgerekende hash van dat bericht, weet je dat dit bericht met

de private key van de verzender is ondertekend en dus niet aangepast. Want niemand anders dan de verzender bezit die private key.

De oplossing:

Om iedere VISI Leverancier nu toch de XAdES ondertekening te laten uitvoeren, wijken we met VISI 1.7 af van de eIDAS certificaat eis af.
Dit doen we door een lijst met vertrouwde public keys en de naam/omschrijving ervan onderling bij te houden in een VISI project dat tussen de VISI leveranciers zelf communiceert.
Mocht er een public key wijzigen/ bij komen/verwijderd worden, dan deelt de leverancier van die verzender de gewijzigde “trust list” van die leverancier met de andere leveranciers.
Het is te verwachten dat hier in de toekomst een meer geavanceerdere “PKI” voor in de plaats komt.
Voor het huidige gebruikt voorziet deze VISI oplossing ruimschoots in een snelle, herleidbare en betrouwbare communicatie en vastlegging van deze sleutels.
De uitvoering van dit VISI raamwerk en eventueel de bestandsopbouw van het lijstje dat zo verzonden wordt, bepalen de leveranciers in de komende weken nog onderling.

XAdES compatibility:
Het is wel zo dat als een ontvangende software de public key uit het bericht zelf niet in deze lijst ziet staan, dat de software dan deze public key alsnog aan de eIDAS pki valideert. Op deze manier kunnen we 100% XAdES proof berichten, die hun sleutel bij de EU en niet in bovenstaande lijstje hebben staan, ook valideren.

Bovenstaande uitleg zal ook onderdeel van de VISI Standaard documentatie worden, zodat voor een ieder duidelijk is hoe we als VISI standaard functioneel tot in detail deze XAdES ondertekening gebruiken.

Time stamp server:

Om ook het tijdstip van ondertekenen 100% veilig vast te leggen is een zogenaamde “Time Stamp server” nodig. Door ook hier een met de private key van de time stamp server het tijdstip van versleutelen vast te leggen, is het niet mogelijk om het bericht op een later moment aan te passen. Mocht een software leverancier een aangepast bericht met de zelfde private key later opnieuw willen ondertekenen, dan is dat niet mogelijk, omdat dan de time stamp server nooit een geantidateerd ondertekend tijdstip zal leveren.

Om ook hier de afhankelijkheid van de eIDAS trusted time stamp leveranciers weg te nemen, wijken we hier af van de eisen van XAdES af. Voor VISI 1.7 volstaat het om een onafhankelijke time stamp server te gebruiken. Dus het is toegestaan om een eIDAS proof time stamp server te gebruiken, maar ook een andere onafhankelijke leverancier van time stamps. Het zelf hosten van een time stamp servers is niet toegestaan, omdat dan antidateren mogelijk zou worden.

Voor wat betreft deze laatste beslissing over een onafhankelijke time stamp server heeft TEEC2 bedenktijd aangevraagd of zij het hier ook mee eens zijn.

29 november 2023,

Arne Bruinse.