Erratum

VZVZ Erratumgegevens	
Datum **Volgnr.** **Status**	19 mei 2017 01 definitief
Publicatie Titel	v6.14 Erratum: PKIO/UZI certificaten gaan over naar nieuwe generatie PvE ZIM, PvE GBx Organisatie, IH Berichtauthenticatie UZI, IH EH UZI, IH Security Tokens generiek

Wijzigingshistorie:

RfC	Beschrijving	Erratum volgnr.	Datum
RFC 71719	PKIO/UZI certificaten gaan over naar nieuwe generatie	01	19-5-2017

RfC	71719	**Erratumvolgnr.**	01
Beschrijving	PKIO/UZI certificaten gaan over naar een nieuwe generatie.		
Probleem-stelling	PKIO/UZI certificaten gaan over naar een nieuwe generatie. Certificaatbomen, waaronder PKIo/UZI certificaten zijn 10 jaar geldig. De huidige boom (G21)verloopt in 2020 en er worden reeds certificaten uitgegeven onder de nieuwe boom. In de huidige documentatie wordt gesproken over de G21 certificaten. Deze komen dus per 2020 te vervallen en zullen worden opgevolgd door de G3 (pascertificaten) en de G1 (servercertificaten). De verschillende generaties zullen tot 2020 naast elkaar blijven bestaan.		
Oplossing	Een XIS-leverancier moet alle door het UZI-register uitgegeven certificaten gaan ondersteunen. De eisen en overige teksten in de documentatie zullen generiek worden opgesteld en niet meer spreken over specifieke certificaatbomen.		
Geraakte documenten	PvE ZIM, PvE GBx Organisatie, IH Berichtauthenticatie UZI, IH EH UZI, IH Security Tokens generiek		

Specifieke plaats	Aanduiding	Wijziging
AORTA_GBx_PvE_Organisatie	Eis GBX.IDA.e4080	3) het betreft passen die zijn uitgegeven onder de op dat moment geldende certificaatboom of –bomen. (SHA-256).

AORTA_GBx_PvE_Organisatie	Eis GBX.BVL.e4050	a) passen met SHA-256-certificaten (uitgegeven onder de op het moment geldende certificaatbo(o)m(en)) gelezen en gebruikt kunnen worden;
AORTA_GBx_PvE_Organisatie	Eis GBX.CON.e4110	Zie de eis zoals opgenomen in Bijlage A.
De diverse IH's	n.v.t.	Kleine wijzigingen met betrekking tot de term G21. Overal waar G21 staat moet nu ook G3 voor pascertificaten en G1 voor servercertificaten gelezen worden.

Bijlage A: Herziene eis GBX.CON.e4110.2

GBX.CON.e4110.2	
Het GBx dient UZI/PKIo-servercertificaten van de (verschillende) generatie(s) te ondersteunen zoals beschikbaar wordt gesteld door het UZI-Register ([UZI-Register]). Er moet gebruik worden gemaakt van het SHA-256 ondertekeningsalgoritme.	
Functie	Ondersteunen servercertificaten en ondertekeningalgoritmen.
Scope	GBZ/GBO/GBK/GBP
Karakter	Verplicht
Condities	-
Toelichting	Het UZI-register geeft UZI-servercertificaten uit onder één of meerdere certificaatbomen. In het geval er onder diverse certificaatbomen UZI-servercertificaten wordt uitgegeven, is het zaak om alle servercertificaten uitgegeven onder de diverse certificaatbomen te kunnen ondersteunen. Een GBX-communicatieserver dient te zijn ingericht op het ondertekeningalgoritme SHA-256.
Verificatiewijze	Demo
Voorheen	GBZ·IE·BVL·e07