**How to create mTLS connectivity using \*.harmanota and \*.harmandev Certificates.**

In order to create/test mTLS connectivity using valid certificates please make sure that:

1. Server (NGINX side) uses \*.harmanota.com certificate and key: [\\iltlv-harman\IT\Production documentation\mTLS\harmanota.crt](file:///\\iltlv-harman\IT\Production%20documentation\mTLS\harmanota.crt)
2. Client (browser in this case) uses \*.harmandev.com **PFX** certificate: [\\iltlv-harman\IT\Production documentation\mTLS\harmandev.pfx](file:///\\iltlv-harman\IT\Production%20documentation\mTLS\harmandev.pfx)
3. To create **PFX** certificate following command used:

*openssl pkcs12 -export -out harmandev.pfx -inkey harmandev\_com.key -in harmandev.crt -certfile gd\_bundle-g2-g1.crt*

1. Server uses GoDaddy provided bundle *gd\_bundle-g2-g1.crt :* [*\\iltlv-harman\IT\Production documentation\mTLS\gd\_bundle-g2-g1.crt*](file:///\\iltlv-harman\IT\Production%20documentation\mTLS\gd_bundle-g2-g1.crt)as client certificate.
2. NGINX configuration should look as following:  
   *ssl\_certificate         /etc/nginx/conf.d/ssl/harmanota-combined.crt;*

*ssl\_certificate\_key     /etc/nginx/conf.d/ssl/harmanota.key;*

*ssl\_client\_certificate  /etc/nginx/conf.d/ssl/gd\_bundle-g2-g1.crt;*

*ssl\_verify\_client       on;*

*ssl\_verify\_depth        3;*

**Important:** NGINX ***ssl\_verify\_depth*** *directive depends on number certificates in* ***ssl\_client\_certificate*** chain, in this case:  
 # grep -c BEGIN gd\_bundle-g2-g1.crt

# 3