**Extract from NHS Digital on IT Technical Change Requirements to Support Move to Cloud Technology**

The information below can be found at:

<https://digital.nhs.uk/services/path-to-live-environments/path-to-live-environment-news/news---week-commencing-15-march-2021>

**What will this mean to you?**

This change will improve platform stability, and the overall user experience.  Ahead of the transition, your IT function will need to:

* Make a change to your firewall;
* Apply root certificates;
* If applicable, remove hard coded IP addresses.

See "What Your IT Function Needs to Do" below for further details.  **Please can you pass this onto your relevant IT resources to action.**

**What Your IT Function Needs to Do**

As per previous details provided, you will need to execute the following steps to ensure your continued access to the service - these changes can be done ahead of the cutover:

1. **Firewall changes** - You will need to allow the traffic out from your firewall to the following address range 155.231.9.0/24 to ports 443 and 636. You will also need to allow inbound connectivity from this range to receive logout notifications.  Making these firewalls changes ahead of the cutover will allow you to participate in the connection check described below - **see Pre-Go Live Connectivity Check section**.
   * When making these firewall changes, subject to how your network connections are set-up, you may need to update your routing / NAT configurations to accommodate the new IP range
2. **Root certificates** - if you have explicitly added any of our certificates to any of your trust stores you will also need to ensure you add the new AWS root certificates ahead of the migration.
   * <https://www.amazontrust.com/repository/> - it is recommended all the certificates listed in the Root CA's section are installed in your Live estate
3. **Hard-coded IP addresses** - If you have hard-coded current Live IP addresses in place of **domain name system**(DNS) entries then these will stop working after the cutover and you will need to change **any hard-coded addresses** in advance  If you have hard-coded the IP address of the service in place of DNS entries, you will need to ensure you return to using the DNS entries. This will ensure you are automatically directed to the new service when the transition takes place. The DNS entries required are:
   * Authentication - [gas.national.ncrs.nhs.uk](http://gas.national.ncrs.nhs.uk/)
   * Directory - [ldap.national.ncrs.nhs.uk](http://ldap.national.ncrs.nhs.uk/)
   * Security Broker - [sbapi.national.ncrs.nhs.uk](http://sbapi.national.ncrs.nhs.uk/)
4. The existing client/user certificates will still be valid against the new Live service and no further action is required.

During the cutover weekend, we will be updating DNS to point at the new IP range.  If the instructions above are followed, we do not anticipate any issues. If you do encounter any issues resolving the host names we do recommend you clear down your DNS cache.

During the transition window we anticipate a very small number of users, who have active sessions, may find that they need to re-authenticate again using normal smartcard processes. We have taken steps to minimise the number of users who will be affected in this way by choosing the timing of the transition carefully and by transitioning session data from the old to the new service.

After the cutover:

* If you are using the legacy BT Identity Agent (IA) you will need to restart the identity agent to pick up the DNS Changes.   
  BT IA is no longer supported and we strongly recommended that you upgrade to the latest version which can be downloaded from <http://nww.hscic.gov.uk/dir/downloads/index.html#identity_agent>
* **Key Contact in case of Problems?**
  + If you experience any issues with the CIS Live environment, please report as normal to the National Service Desk (03003 035 035 - [ssd.nationalservicedesk@nhs.net](mailto:ssd.nationalservicedesk@nhs.net)).

Pre-Go Live Connectivity Check - A few weeks ahead of the actual cutover, we would like you to perform a check.  This check will allow you to test your connection to the new Production environment and ensure your firewall changes have been applied (see point 1 Firewall changes below).  If you experience any issues or would like some advice/guidance please contact (SPINECIS, Sm (NHS DIGITAL) [sm.cellone@nhs.net](mailto:sm.cellone@nhs.net)).  This check will only be available for a limited period of time between **Monday 19 April (BST) 09:00 to Monday 26 April (BST) 18:00**:

1. You will be able to check the connectivity to the new AWS platform using the following hostnames (see specific instructions below).
   1. <https://gas.prod.cis.spine2.ncrs.nhs.uk/>
   2. <https://sbapi.prod.cis.spine2.ncrs.nhs.uk/>
   3. ldap.prod.cis.spine2.ncrs.nhs.uk

* You can test connectivity to the gas and sbapi services using either a web browser or a command line utility such as curl, A successful connection will return the static response "Welcome to CIS"

|  |
| --- |
| *curl*[*https://gas.prod.cis.spine2.ncrs.nhs.uk/*](https://gas.prod.cis.spine2.ncrs.nhs.uk/)  *Welcome to CIS* |

* You can test the connectivity to the ldap service by using the openssl command line utility and your existing ldap client certificates

|  |
| --- |
| *openssl s\_client -connect ldap.prod.cis.spine2.ncrs.nhs.uk:636 -servername ldap.prod.cis.spine2.ncrs.nhs.uk -CAfile root.pem -cert yourcert.crt -key yourcert.key* |

* If you are able to connect successfully you should see a response similar to the following.

|  |
| --- |
| *CONNECTED(00000005)*  *depth=2 O = nhs, OU = CA, CN = NHS PTL Root Authority*  *verify return:1*  *depth=1 O = nhs, OU = CA, CN = NHS DEV Level 1C*  *verify return:1*  *depth=0 O = nhs, OU = Devices, CN = ldap.vn03.national.ncrs.nhs.uk*  *verify return:1*  *---*  *Certificate chain*  *0 s:O = nhs, OU = Devices, CN = ldap.vn03.national.ncrs.nhs.uk*  *i:O = nhs, OU = CA, CN = NHS DEV Level 1C*  *1 s:O = nhs, OU = CA, CN = NHS DEV Level 1C*  *i:O = nhs, OU = CA, CN = NHS PTL Root Authority*  *2 s:O = nhs, OU = CA, CN = NHS PTL Root Authority*  *i:O = nhs, OU = CA, CN = NHS PTL Root Authority*  *---*  *Server certificate*  *-----BEGIN CERTIFICATE-----*  *MIIEETCCAvmgAwIBAgIEXa24TjANBgkqhkiG9w0BAQsFADA2MQwwCgYDVQQKEwNu*  *aHMxCzAJBgNVBAsTAkNBMRkwFwYDVQQDExBOSFMgREVWIExldmVsIDFDMB4XDTE5*  *MTExNDE0NTMyMloXDTIyMTExNDE1MjMyMlowSTEMMAoGA1UEChMDbmhzMRAwDgYD*  *VQQLEwdEZXZpY2VzMScwJQYDVQQDEx5sZGFwLnZuMDMubmF0aW9uYWwubmNycy5u*  *aHMudWswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDkQXs+JW/u3PkL*  *uoOglALsQlkTVUZUkPWf+KYmrNZdtnx2hD0Y7fclvWH0ZkJHfnwD632hW+fDTiZc*  *mM0/wx9P1DkAG/l06fStAcWTEIAES3/eIipSCORbmF4O2+HvXkRMRrs+jRKZJuwq*  *2/umGMC5MODM0NIbT21F7O7r9czv/k7yzcZEljqRv6V9TvMvwbCzUR39LiYEuTLE*  *M0h5MtISshlmh60xu9BGNelLhL7GEIXsQwkIxnAfOSzqXdb58pNY6VVSx6JphndS*  *5U3SHa3oYcEfSPB7/q77K5UnCm+yy0KCVnFEoXUpO3DLx4IdZi9v+2iTmkUPzryH*  *0mGhYCNlAgMBAAGjggESMIIBDjALBgNVHQ8EBAMCBaAwHQYDVR0lBBYwFAYIKwYB*  *BQUHAwEGCCsGAQUFBwMCMBgGA1UdIAQRMA8wDQYLKoY6AIl7ZQADAQEwMwYDVR0f*  *BCwwKjAooCagJIYiaHR0cDovL2NybC5uaHMudWsvZGV2LzFjL2NybGMxLmNybDAr*  *BgNVHRAEJDAigA8yMDE5MTExNDE0NTMyMlqBDzIwMjExMjIwMjAxMTIyWjAfBgNV*  *HSMEGDAWgBRe89pS9gIu2pomUlH/STXIDHcNdjAdBgNVHQ4EFgQU6drAg31Mxhqx*  *UnihdN9RUjbAMdowCQYDVR0TBAIwADAZBgkqhkiG9n0HQQAEDDAKGwRWOC4zAwIE*  *sDANBgkqhkiG9w0BAQsFAAOCAQEAOrrWGAWH3D4C2SbvDNx4bpAzHYyRefVg/zIZ*  *um/wOLjkQ6n7lN7VgkVJrmQkahrgbQvtlLfZdZcJ3T8qkLcSwfZaIR6Bfl6L9Pqa*  *DjYbLLeRtvC6LCiLTSOt143JQ0SD1HvvbzNa6PLqem7qfpQvOzwbCmJ8x/p5Njqw*  *QFaJyZgcxiHetUmaFLjez+TG1n5AppMOvLxZjW0XXgPzPoCmjIUzJZtm+0ThyAOP*  *y3nm6TbDGaDxymuVHdsQ1v9dxa/6uD7hekkqedAvpJb9smVrrZH4hc2gmrYBhmu8*  *hhQZBHNPQW3qqyK7Bnje7CHwZicWl7UfbBHTsmDvYmtoliQjrQ==*  *-----END CERTIFICATE-----*  *subject=O = nhs, OU = Devices, CN = ldap.vn03.national.ncrs.nhs.uk*  *issuer=O = nhs, OU = CA, CN = NHS DEV Level 1C*  *---*  *Acceptable client certificate CA names*  *O = nhs, OU = CA, CN = VNIS03\_SUBCA*  *O = nhs, OU = CA, CN = VNIS03\_RootCA*  *O = nhs, OU = CA, CN = NHS PTL Root Authority*  *O = nhs, OU = CA, CN = NHS DEV Level 1C*  *Requested Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA224:ECDSA+SHA1:RSA+SHA224:RSA+SHA1*  *Shared Requested Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512*  *Peer signing digest: SHA256*  *Peer signature type: RSA-PSS*  *Server Temp Key: X25519, 253 bits*  *---*  *SSL handshake has read 3772 bytes and written 3615 bytes*  *Verification: OK*  *---*  *New, TLSv1.3, Cipher is TLS\_AES\_256\_GCM\_SHA384*  *Server public key is 2048 bit*  *Secure Renegotiation IS NOT supported*  *Compression: NONE*  *Expansion: NONE*  *No ALPN negotiated*  *Early data was not sent*  *Verify return code: 0 (ok)*  *---*  *---*  *Post-Handshake New Session Ticket arrived:*  *SSL-Session:*  *Protocol  : TLSv1.3*  *Cipher    : TLS\_AES\_256\_GCM\_SHA384*  *Session-ID: B2A21E7CC0E50DD140016FE26D7E31D0CAF07702871CA0AFFA1933A30D9D1312*  *Session-ID-ctx:*  *Resumption PSK: C9360EE2D60A99DA7CF23567A59926389F9266BD516A38E406AB39B1ACDE230B5EA4A4CCA1FC7DB8D5187B1D897AB01F*  *PSK identity: None*  *PSK identity hint: None*  *SRP username: None*  *TLS session ticket lifetime hint: 7200 (seconds)*  *TLS session ticket:*  *0000 - 9f 6c 14 11 7b 30 28 c4-7c 5d 34 36 29 ab 55 45   .l..{0(.|]46).UE*  *0010 - 57 2b 8b b8 f0 a0 a0 de-73 62 d7 c0 d9 a2 af 92   W+......sb......*  *Start Time: 1615552335*  *Timeout   : 7200 (sec)*  *Verify return code: 0 (ok)*  *Extended master secret: no*  *Max Early Data: 0*  *---*  *read R BLOCK*  *---*  *Post-Handshake New Session Ticket arrived:*  *SSL-Session:*  *Protocol  : TLSv1.3*  *Cipher    : TLS\_AES\_256\_GCM\_SHA384*  *Session-ID: CD9ED1F09D66A55264E69DB2B2D8A1ED871DBE3D1D53125ADBD617B1DAF34EC0*  *Session-ID-ctx:*  *Resumption PSK: 8F4E2CD679E77FC20CEA1782B74404ED3EA4038BEB5E265FBC9A2531C33A6B73891CDAD548DC19E88D65AF70752ADBE7*  *PSK identity: None*  *PSK identity hint: None*  *SRP username: None*  *TLS session ticket lifetime hint: 7200 (seconds)*  *TLS session ticket:*  *0000 - b4 3c d0 2a cf ce ac 5e-95 f2 3b fa 55 e1 b7 b9   .<.\*...^..;.U...*  *0010 - 50 3e 9a 0f 09 cd 79 50-e0 a2 91 4e 23 6a 60 06   P>....yP...N#j`.*  *Start Time: 1615552335*  *Timeout   : 7200 (sec)*  *Verify return code: 0 (ok)*  *Extended master secret: no*  *Max Early Data: 0*  *---*  *read R BLOCK* |

**Other Information**

In line with general security recommendations, CIS will no longer support SSL - only TLSv1 (and above) will be supported.  If you are using SSL v2 or SSL v3 then**you will need to** **upgrade to later versions of TLS** before the CIS Live transition date.   If you are using SSL, please can you directly contact (SPINECIS, Sm (NHS DIGITAL) [sm.cellone@nhs.net)](mailto:sm.cellone@nhs.net))) urgently.