

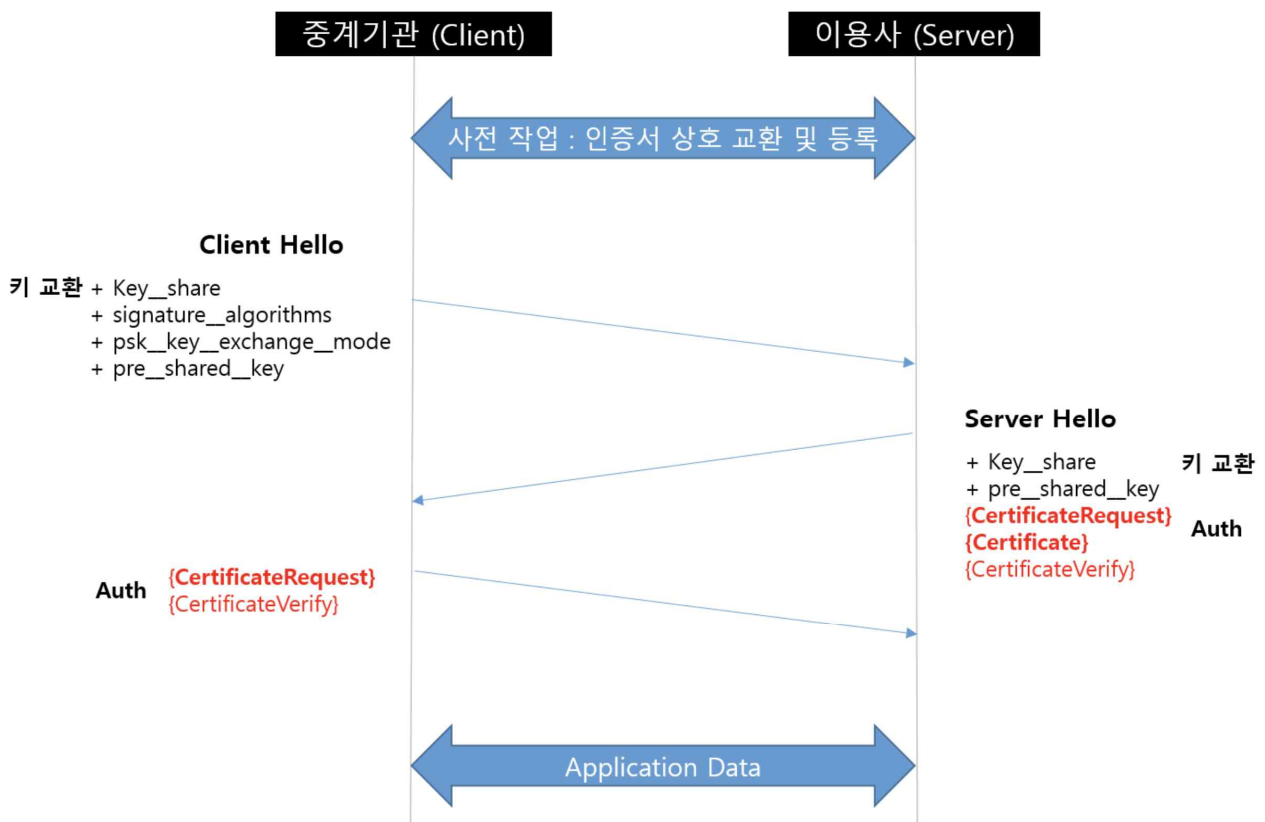
# 코스콤 중계기관 이용자 mTLS 가이드

(21.08.17 코스콤)

※ 본 문서는 중계기관과 이용자 간 개인신용정보 전송을 위해 mTLS(Mutual TLS)를 이용하여 통신하는 방안 기술

## □ mTLS 개요

- 기존 TLS 1.3 절차에서 클라이언트의 인증서 제출 및 검증을 포함하여 상호인증을 수행하는 TLS 흐름도



## □ mTLS 필요성 및 장단점

- **(필요성)** 마이데이터 업무 특성상 중계기관과 이용자 간 개인신용정보 (민감정보) 송수신이 발생하며 이를 위한 보안상의 정책 수립 필요
  - 민감정보인 개인신용정보 송수신을 위해 상호 인지된 서버들 간의 통신을 위해 mTLS 사용
- **(장점)** 상호 인증 된 서버간의 통신이 가능하므로 HMAC과 같은 추가적인 검증절차 없이 표준 절차를 따름으로써 보안요건 충족
- **(단점)** 상호인증을 위해 별도의 인증서 관리 필요

## □ mTLS 인증서 규격

- **(이용대상)** '인터넷공중망 + HTTPS [mTLS]' 로 중계기관과 연결하는 이용자만 해당
  - ※ '인터넷공중망+VPN' 로 네트워크 연계하는 이용자의 경우 미해당
- **(인증서 규격)** Trusted CA에서 발급한 OV등급 TLS인증서
  - 등급 : OV (Organization Validation)
  - Trusted CA 기준 : Microsoft Included CA 인증서 목록\* 참조
    - \* MS Trusted CA 목록 :  
<https://ccadb-public.secure.force.com/microsoft/IncludedCACertificateReportForMSFT>
  - TLS 버전 : TLS 1.3 이상
    - ※ Wildcard 인증서 사용 가능
    - ※ 중계기관에서 Hostname Verification을 적용할 예정이므로 인증서의 주체 이름(CN)과 이용자 접속서버의 hostname은 동일해야 함

## ○ (중계기관 TLS인증서 정보)

- 인증서 도메인 : \*.k-mydata.org
- 인증서 인증기관 : digicert
- 중계기관 TLS인증서 다운로드 경로

### 1) 현재인증서(current) :

[https://cdn.k-mydata.org/public/certs/current/wildcard\\_k-mydata\\_org.pem](https://cdn.k-mydata.org/public/certs/current/wildcard_k-mydata_org.pem)

### 2) 갱신인증서(latest) :

[https://cdn.k-mydata.org/public/certs/latest/wildcard\\_k-mydata\\_org.pem](https://cdn.k-mydata.org/public/certs/latest/wildcard_k-mydata_org.pem)

※ 갱신인증서는 현재인증서 만료일 30일 전 업데이트 되며 만료일 이후에는 현재인증서와 동일

## □ mTLS 수립을 위한 사전 절차

- 1) 네트워크 연결 (인터넷망 연결)
- 2) 이용자 서버의 접속주소(FQDN) 준비 및 중계기관으로 전달
- 3) '이용사 TLS인증서' 발급 및 전달
  - (발급) 이용자 TLS인증서\* 발급
  - \* 기존 TLS인증서를 보유한 경우 이를 활용 가능
  - (전달) 발급받은 이용자 TLS인증서를 오프라인, 이메일 등을 활용하여 중계기관으로 전달
- 4) '중계기관 TLS인증서' 수신 및 등록
  - (수신) 중계기관 TLS인증서 다운로드
  - (등록) 중계기관 TLS인증서를 이용자측 Trust Store에 등록하여 인증서를 검증 또는 중계기관 TLS인증서 CA(Certificate Authority)를 통한 검증

※ TLS인증서 전달 포맷 : 웹서버용 TLS인증서 FullChain: PEM<sup>1)</sup> 파일

1) PEM : Privacy Enhanced Mail

## 5) 추가 보안 요소 적용

### - (시스템별 보안 요소 적용 기준)

| 이용사<br>시스템 구분      | 추가 보안 요소<br>적용 기준 | 비고                |
|--------------------|-------------------|-------------------|
| 가동                 | 필수                | IP접근제어 및 CN값검증 필수 |
| Staging<br>테스트(개발) | 권고                | IP접근제어 및 CN값검증 권고 |

### - (IP접근제어) 중계기관의 IP에 대해서만 접속을 허용하도록 IP를 Whitelist\*로 관리

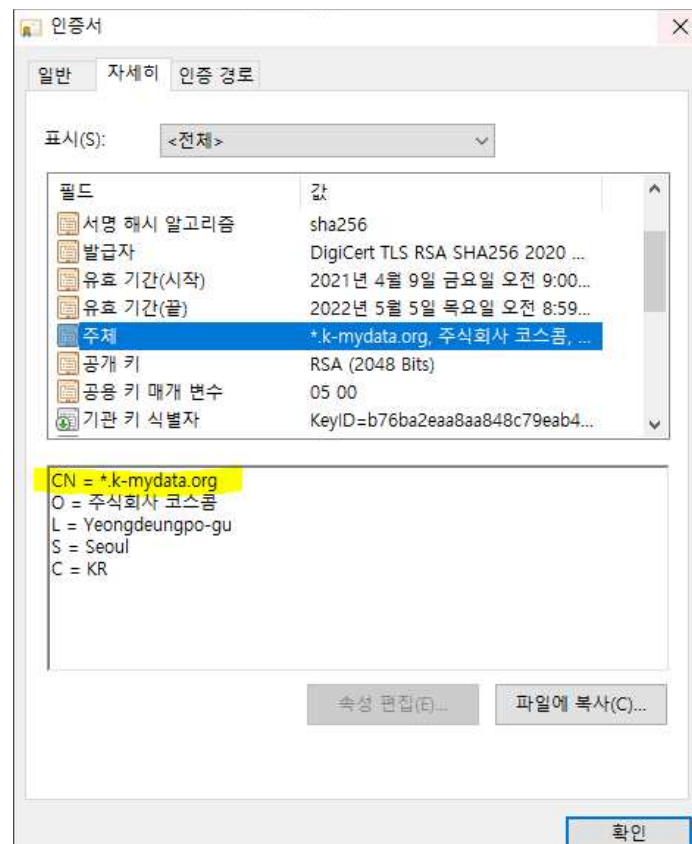
\* 허용목록에 있는 IP 이외에 모든 접속을 금지하는 형태의 보안요소

| 중계기관<br>시스템 구분 | 중계기관<br>Outbound IP 주소 | 비고                     |
|----------------|------------------------|------------------------|
| 가동             | 221.168.35.137         | 이용사 가동시스템 접근설정용        |
| 샌드박스           | 221.168.35.138         | 이용사 Staging시스템 접근설정용** |
| 테스트(개발)        | 221.168.35.159         | 이용사 테스트시스템 접근설정용       |

\*\* 이용자 Staging시스템이 없을 경우 이용자 테스트시스템을 연계

### - (CN값 검증) 중계기관이 접속 시 전달한 인증서의 내용 중 CN값이 '\*.k-mydata.org' 인지 확인

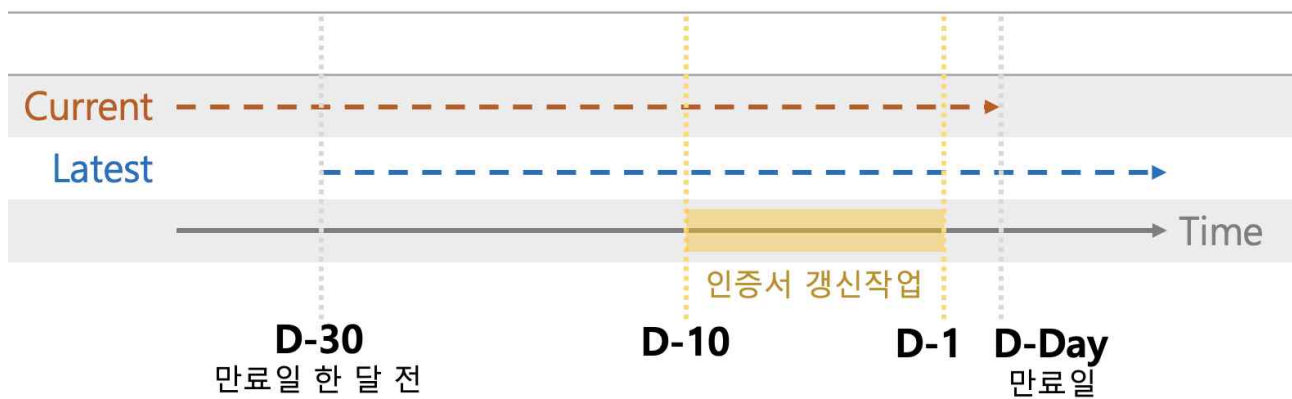
※ 인증기관(CA)에서 검증된 도메인 주소로, 중계기관만 가지는 유일한 값



## □ TLS인증서 상태 관리

- 서비스 연속성을 위해 이용자 및 중계기관은 상호 TLS인증서 상태 관리 필요
- 인증서 유효기간 만료일 **최소 한 달 전** 상호간 인증서갱신 사전 고지
- (이용사 TLS인증서 갱신)
  - (전달) 갱신된 이용자 TLS인증서와 적용예정일자를 중계기관으로 전달
    - ※ 이용자 TLS인증서 만료일 **최소 한 달 전** 고지
- (중계기관 TLS인증서 갱신)
  - 1) [만료일 1달 전] 갱신된 중계기관 TLS인증서(갱신인증서;latest) 다운로드
  - 2) [만료일 1달 전 ~ 만료일] 중계기관 TLS 인증서(현재인증서;current) 만료일까지 이용자 측 Trust Store에 현재인증서와 갱신인증서 둘 다 보관
  - 3) [만료일 10일 전 ~ 만료일 1일 전] 중계기관이 TLS인증서 교체작업 수행
  - 4) [만료일] 갱신된 중계기관 TLS인증서만 이용 가능

[중계기관 TLS인증서 유효기간]



## □ 이용자측 서버 mTLS 설정 샘플

- 이용자 측 서버 Web Server 또는 Application level 에서 ‘중계기관 TLS인증서’ 등록 및 검증 필요

### - Web Server 설정 예시 (NGINX Example)

```
map $ssl_client_s_dn $ssl_client_s_dn_cn {
    default "";
    ~(^|,)CN=(?<CN>[^,]+) $CN;
}
server {
    listen 443 ssl;
    ssl on;
    server_name testmydata.server.com;
    ssl_certificate      /{path}/server.crt;
    ssl_certificate_key  /{path}/server.key;
    ssl_protocols TLSv1.3;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_client_certificate /{TrustStorePath}/client.crt; //truststore
    ssl_verify_client on;
    ...
    location / {
        if ($ssl_client_verify != SUCCESS) { return 403; }
        <!-- verify CN in client certificates -->
        if ($ssl_client_s_dn_cn !~ "k-mydata.org") { return 401; }
    }
}
```

### - Application 설정 예시 (JAVA JSSE Example)

*\* min JDK8, import bouncy castle library*

```
private static String[] protocols = new String[] { "TLSv1.3" };
private static String[] cipher_suites = new String[] { "TLS_AES_128_GCM_SHA256" };

//set TrustStore
System.setProperty("javax.net.ssl.trustStore", "\\PATH\\keytool\\client.jks");
System.setProperty("javax.net.ssl.trustStorePassword", "passwd123");
System.setProperty("javax.net.ssl.trustStoreType", "JKS");

public static SSLSocket create(String hostname, int port) throws IOException {
    SSLServerSocket sslServerSocket =
        (SSLServerSocket) SSLServerSocketFactory.getDefault().createServerSocket(port);
    SSLSocket sslSocket = (SSLSocket) sslServerSocket.accept();

    sslSocket.setHandshakeApplicationProtocolSelector(
        (serverSocket, clientProtocols) -> {
            //extract CN in certificates during the handshake
            SSLSession handshakeSession = serverSocket.getHandshakeSession();
            X509Certificate[] certs = handshakeSession.getPeerCertificateChain();
            X509Name x500name = new JcaX509CertificateHolder(certs[0]).getSubject();
            RDN cnRdn = x500name.getRDNs(BCStyle.CN)[0];
            String cn = IETFUtils.valueToString(cnRdn.getFirst().getValue());
            if(!cn.equals("*.k-mydata.org"))
                throw new SSLHandshakeException("CN doesn't match hostname");
            return chooseApplicationProtocol(
                serverSocket, clientProtocols, handshakeSession.getProtocol(),
                handshakeSession.getCipherSuite());
        });
    sslSocket.startHandshake();
    sslSocket.setEnabledProtocols(protocols);
    sslSocket.setEnabledCipherSuites(cipher_suites);
    sslSocket.setNeedClientAuth(true);
}
```

## TLS인증서 FullChain 파일 예시 (.pem형식)

|    |  |
|----|--|
| 양식 | <pre> -----BEGIN CERTIFICATE----- (Your Primary SSL certificate: your_domain_name.crt) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- (Your Intermediate certificate: DigiCertCA.crt) -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- (Your Root certificate: TrustedRoot.crt) -----END CERTIFICATE----- </pre>   |
| 샘플 | <pre> -----BEGIN CERTIFICATE----- KOSCOMPRIMARYwIBAgIBADkoscomhkiG9w0BAQQFADBXMqswCQYDVQQGEwJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1koscom VU4xFDASBgNVBAMTC0hlcm9uZyZyZW5nMB4XDTA1MDcxNTIxMTk0N1oXDTA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTAIBOMQswCQYDVQQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTAIVOMRQwEgYDVQQDEwltZXJvbmVmcGWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBewKE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbM0oRcKK9vEcGmtcLFuQTWDI3RagMBAAGj gbEwga4wHQYDVR00BBYEFFXI70krkoscomgbaCQoR4jUDncEMH8GA1koscomMHAA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMqswCQYDVQQGEwJDTjELMAkGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECXMVCVU4xFDAS BgNKOSCOM0hlcm9uZyZyZW5nggEAMAwGA1UdEwQFMAMBAf8wDkoscomIhvcNAQEE BQADQQA/ugzBrjK9jcWnDVfGHIk3icNRq0oV7Ri32z/+HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQ0msPue9777lx -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- IntermediateICA1234koscomhkiG9w0BAQQFADBXMqswCQYDVQQGEwJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1koscom VU4xFDASBgNVBAMTC0hlcm9uZyZyZW5nMB4XDTA1MDcxNTIxMTk0N1oXDTA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTAIBOMQswCQYDVQQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTAIVOMRQwEgYDVQQDEwltZXJvbmVmcGWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBewKE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbM0oRcKK9vEcGmtcLFuQTWDI3RagMBAAGj gbEwga4wHQYDVR00BBYEFFXI70krkoscomgbaCQoR4jUDncEMH8GA1koscomMHAA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMqswCQYDVQQGEwJDTjELMAkGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECXMVCVU4xFDAS BgNKOSCOM0hlcm9uZyZyZW5nggEAMAwGA1UdEwQFMAMBAf8wDkoscomIhvcNAQEE BQADQQA/ugzBrjK9jcWnDVfGHIk3icNRq0oV7Ri32z/+HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQ0msPue9rsagO -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOTCA123456AwIBAgIBADkoscomhkiG9w0BAQQFADBXMqswCQYDVQQGEwJDTjEL MAkGA1UECBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1koscom VU4xFDASBgNVBAMTC0hlcm9uZyZyZW5nMB4XDTA1MDcxNTIxMTk0N1oXDTA1MDgx NDIxMTk0N1owVzELMAkGA1UEBhMCQ04xCzAJBgNVBAGTAIBOMQswCQYDVQQHEwJD TjELMAkGA1UEChMCT04xCzAJBgNVBAsTAIVOMRQwEgYDVQQDEwltZXJvbmVmcGWWFu ZzBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCp5hnG7ogBhtlynpOS21cBewKE/B7j V14qeyslnr26xZUsSVko36ZnhiaO/zbM0oRcKK9vEcGmtcLFuQTWDI3RagMBAAGj gbEwga4wHQYDVR00BBYEFFXI70krkoscomgbaCQoR4jUDncEMH8GA1koscomMHAA FFXI70krXeQDxZgbaCQoR4jUDncEoVukWTBXMqswCQYDVQQGEwJDTjELMAkGA1UE CBMCUE4xCzAJBgNVBACtAkNOMQswCQYDVQQKEwJPTjELMAkGA1UECXMVCVU4xFDAS BgNKOSCOM0hlcm9uZyZyZW5nggEAMAwGA1UdEwQFMAMBAf8wDkoscomIhvcNAQEE BQADQQA/ugzBrjK9jcWnDVfGHIk3icNRq0oV7Ri32z/+HQX67aRfgZu7KWdI+Ju Wm7DCfrPNGVwFWUQ0msPue9rZbb1 -----END CERTIFICATE----- </pre> |