Key rollover in FedTLS

Found an error? Please contact info@skolfederation.se for correction.

Introduction

Key rollover, or certificate rollover, is used when needed to change security certificates and keys in services. This guide presents an alternative for changing keys for a client or server in a FedTLS federation.

FedTLS supports declaring and using multiple keys, which can be used for a smooth rollover of keys to eliminate downtime for clients and servers in the federation.

Overview

Here is a brief overview of the steps taken to achieve the key rollover:

- A FedTLS entity in Moa declares a public key pin (PKP) corresponding to a certificate that needs to be changed. The entity declares the corresponding issuer certificate(s) for the entity PKP to support reverse proxy applications validating the chain of trust when required. For changing keys there are two scenarios:
    - The member enrolls a new certificate with a corresponding new PKP based on the entity's existing published issuer(s) in the metadata. The new PKP is published in the federation metadata alongside the old PKP to achieve a smooth rollover.
    - The member creates a new self-signed certificate with a corresponding new PKP. The new PKP for the self-signed certificate is published in the federation metadata alongside the old PKP to achieve a smooth rollover. The self-signed certificate also has to be added as an issuer certificate in the entity metadata to maintain the chain of trust.
- After new values are added and uploaded to the certificate the relying federation entities will automatically add the new certificate information to their respective trust stores. When this is done, key rollover can be done in the federation service, and if successful the old key values can be removed from the entity metadata.

Web certificates with a chain of trust rooting from a public web certificate authority is not required, nor recommended, as the chain of trust is established by the federation metadata and trust framework.

Key rollover in FedTLS

Current metadata with old PKP

Below is an example metadata for a client. It has its public key pin declared in the "pins" array, and the entity's issuer certificate is declared in the "issuers" array.

MD with old PKP


```
{
  "version": "1.0.0",
  "entities": [
    {
      "entity_id": "https://example.com",
      "organization": "Example Organization",
      "organization_id": "SE999999999901",
      "issuers": [
        {
          "x509certificate": "-----BEGIN CERTIFICATE-----
\nMIIFDzCCAvegAwIBAgIJAOT8hEFzAhWpMA0GCSqGSIb3DQEBCwUAMB0xGzAZBgNV\nBAMMEkludGVybmV0c3RpZnRlbHNlbjAgFw0xOTEyMDQx
MjA2MzBaGA8yMTU2MTAy\nNjEyMDYzMFowHTEbMBkGA1UEAwwSSW50ZXJuZXRzdGlmdGVsc2VuMIICIjANBgkq\nhkiG9w0BAQEFAAOCAg8AMIIC
CgKCAgEAvFjSuM20KDstYzCyaFGIxnLKALWxNSF7\nOxEnQLllW4Rr7wmKL7RFSza4wNZGPfJ/MUZC
/lZllwxYigdWbylTjPLdlu4iFyFy\n0lhAUmp5ffoMOi3V+E6pNpQ3RAfvud47mgmtDH2N4MP+Guvy6q5klCwqjC1XDaF+\nXd+hzWi0Wl+6d1E
/Bx9zaYTY6AaYGVXAeKUpnjDycHIW1q48KDCYJyciaBEFbvpG\nD7lPSPXeDrl1Y1Yl/X8zGM
/7oRxX2JG8GI1OJcS5jhIzA6QXjxXaLd7lcg2TW343\n/iefieVw/vJ+ZrPxh+g/9oW+L+oke5WOoKN7gBVy
/pEfJXk+BDc2LFFqAfP3oJeN\nmi3ytwIAATDsN8/5cF/+k/iERSaRnauzDJ7jwRr8wjBdjqUKKCyIhesACz8bw
/+i\noDZSVP2aMEJOUK0fPhhwcQMrk7C8EiixjsD53xaGX4DSjRH93klf84q1vUfmJ++z\n5uvtP4ESXd4YAde4G+DFTYeQGHA6zUx9c7lB7CPbr
5ZP1cS5YtdnWgY7vdfjzZWQ\nCboWy9oLYEQt8hZ1L0qkyqxT83ryj/0GE39vycXAGTB5fgUTCarl2HEQx1mBWAcN\neZrbw6/Ga
/e7UGSgVX6eV0IzyaQBSdRTqnNDqs0YGce4jqVmYMQnI+ntTtMMLK+N\n1AAphfH++gsCAwEAAaNQME4wHQYDVR0OBBYEFMbCO7AoA1kZvqKN0TV
4vLClBNM1\nMB8GA1UdIwQYMBaAFMbCO7AoA1kZvqKN0TV4vLClBNM1MAwGA1UdEwQFMAMBAf8w\nDQYJKoZIhvcNAQELBQADggIBAHxc4KJiU9k
9bMAqYBX72EsWfFz5SlE8ACnGixSq\nh7Zw8sT97X6URJkiDu8DhoHAA1rKxYZbIeIYSJIJleodltR7Q0LgPyEyBay1GEWX\ndq1CteIFjChtYjA
j/S9xDQP3/M5THQDuH2ATOc7szwWg13u
/8S3l4siA6nPvR6tr\nqYFQK5MrhrLvkAEpJ814qIw4zspT9lrxcALad4M+dUh0UoqF5cFcAaPcRm68N6xN\nfzaDOBSCZWMO2fd7lRvBYK+NREu
2ebuz9wG/ChcKLBuShEaKHkpzPNoEp+sZuiYR\n5q8F6wjA/vFXBaRacSTmRSwHS/fPojVjDgjWlsGKZRYeqvexdiJV0npYdb
/k9x0j\nKk8omjaJT9+yGCliS82/Bszar4vZoonoR5g+XC+
/oDw4tx48dPvW+6hbI7PNbdRI\nasZJTlDfvyavu7dhUm3c90ZiqcpBbDJu1AVtfI5eoQ59WgDUdlTMH2fHY8+q38w3\nAsRVYKB+bNXtfJnt4S6
kWN3DGBhaoubY7oOBLD/IT3NU9CmPHVKV0UwlYpohUyWs\nvOMl8lRlKinOkvpv79C0KYzsN9EwbBsAkS1noxI8Z9m4ySljpfEmqVg1CF7t
/E86\nhr1pq6cgZyrOKVWwNdvaKJ/RTET+HbMY+ytzV9dY+tB7ZA8GFw/yFhuJ386KtsNG\n3imj\n-----END CERTIFICATE-----"
        }
      ],
      "clients": [
        {
          "description": "Example Client",
          "pins": [
            {
              "alg": "sha256",
              "digest": "lLHff44448neMMYbdh2dfaLknCLM4xJe/FaXI/Q5Dcs="
            }
          ],
          "tags": ["exampletag"]
        }
      ]
    }
  ]
}
```


The certificate used by the client for establishing the TLS connections needs to be changed, and so we need to add a new corresponding PKP to the "pins". Also, if required, the corresponding issuer certificate is added to "issuers". In case the certificate is self-signed, the new self-signed certificate is added to "issuers".

MD with old and new keys to be published


```
{
  "version": "1.0.0",
  "entities": [
    {
      "entity_id": "https://example.com",
      "organization": "Example Organization",
      "organization_id": "SE999999999901",
      "issuers": [
        {
          "x509certificate": "-----BEGIN CERTIFICATE-----\nMIIFDzCCAvegAwIBAgIJAOT8hEFz.... old cert issuer....
AhWpMA0GCSqGSIb3DQEBCwUAMB0xGzAZBgNV\nBAMMEkludGVybmV0c3EyMDQxMjA2MzBaGA8yMTU2MTAy\nNjEyMDYzMFowHTEbMBkGA1UEAwwS
```

```
SW50ZXJuZXRzdGlmdGVsc2VuMIICIjANBgkq\nhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvFjSuM20KDstYzCyaFGIxnLKALWxNSF7\nOxEnQLll
W4Rr7wmKL7RFSza4wNZGPfJ/MUZC
/lZllwxYigdWbylTjPLdlu4iFyFy\n0lhAUmp5ffoMOi3V+E6pNpQ3RAfvud47mgmtDH2N4MP+Guvy6q5klCwqjC1XDaF+\nXd+hzWi0Wl+6d1E
/Bx9zaYTY6AaYGVXAeKUpnjDycHIW1q48KDCYJyciaBEFbvpG\nD7lPSPXeDrl1Y1Yl/X8zGM
/7oRxX2JG8GI1OJcS5jhIzA6QXjxXaLd7lcg2TW343\n/iefieVw/vJ+ZrPxh+g/9oW+L+oke5WOoKN7gBVy
/pEfJXk+BDc2LFFqAfP3oJeN\nmi3ytwIAATDsN8/5cF/+k/iERSaRnauzDJ7jwRr8wjBdjqUKKCyIhesACz8bw
/+i\noDZSVP2aMEJOUK0fPhhwcQMrk7C8EiixjsD53xaGX4DSjRH93klf84q1vUfmJ++z\n5uvtP4ESXd4YAde4G+DFTYeQGHA6zUx9c7lB7CPbr
5ZP1cS5YtdnWgY7vdfjzZWQ\nCboWy9oLYEQt8hZ1L0qkyqxT83ryj/0GE39vycXAGTB5fgUTCarl2HEQx1mBWAcN\neZrbw6/Ga
/e7UGSgVX6eV0IzyaQBSdRTqnNDqs0YGce4jqVmYMQnI+ntTtMMLK+N\n1AAphfH++gsCAwEAAaNQME4wHQYDVR0OBBYEFMbCO7AoA1kZvqKN0TV
4vLClBNM1\nMB8GA1UdIwQYMBaAFMbCO7AoA1kZvqKN0TV4vLClBNM1MAwGA1UdEwQFMAMBAf8w\nDQYJKoZIhvcNAQELBQADggIBAHxc4KJiU9k
9bMAqYBX72EsWfFz5SlE8ACnGixSq\nh7Zw8sT97X6URJkiDu8DhoHAA1rKxYZbIeIYSJIJleodltR7Q0LgPyEyBay1GEWX\ndq1CteIFjChtYjA
j/S9xDQP3/M5THQDuH2ATOc7szwWg13u
/8S3l4siA6nPvR6tr\nqYFQK5MrhrLvkAEpJ814qIw4zspT9lrxcALad4M+dUh0UoqF5cFcAaPcRm68N6xN\nfzaDOBSCZWMO2fd7lRvBYK+NREu
2ebuz9wG/ChcKLBuShEaKHkpzPNoEp+sZuiYR\n5q8F6wjA/vFXBaRacSTmRSwHS/fPojVjDgjWlsGKZRYeqvexdiJV0npYdb
/k9x0j\nKk8omjaJT9+yGCliS82/Bszar4vZoonoR5g+XC+
/oDw4tx48dPvW+6hbI7PNbdRI\nasZJTlDfvyavu7dhUm3c90ZiqcpBbDJu1AVtfI5eoQ59WgDUdlTMH2fHY8+q38w3\nAsRVYKB+bNXtfJnt4S6
kWN3DGBhaoubY7oOBLD/IT3NU9CmPHVKV0UwlYpohUyWs\nvOMl8lRlKinOkvpv79C0KYzsN9EwbBsAkS1noxI8Z9m4ySljpfEmqVg1CF7t
/E86\nhr1pq6cgZyrOKVWwNdvaKJ/RTET+HbMY+ytzV9dY+tB7ZA8GFw/yFhuJ386KtsNG\n3imj\n-----END CERTIFICATE-----"
        },
        {
          "x509certificate": "-----BEGIN CERTIFICATE-----\nMIIFDzCCAvegAwIBAgIJAOT8hEFz.... new cert issuer....
8AMIICCgKCAgEAvFjSuM20KDstYzCyaFGIxnLKALWxNSF7\nOxEnQLllW4Rr7wmKL7RFSza4wNZGPfJ/MUZC
/lZllwxYigdWbylTjPLdlu4iFyFy\n0lhAUmp5ffoMOi3V+E6pNpQ3RAfvud47mgmtDH2N4MP+Guvy6q5klCwqjC1XDaF+\nXd+hzWi0Wl+6d1E
/Bx9zaYTY6AaYGVXAeKUpnjDycHIW1q48KDCYJyciaBEFbvpG\nD7lPSPXeDrl1Y1Yl/X8zGM
/7oRxX2JG8GI1OJcS5jhIzA6QXjxXaLd7lcg2TW343\n/iefieVw/vJ+ZrPxh+g/9oW+L+oke5WOoKN7gBVy
/pEfJXk+BDc2LFFqAfP3oJeN\nmi3ytwIAATDsN8/5cF/+k/iERSaRnauzDJ7jwRr8wjBdjqUKKCyIhesACz8bw
/+i\noDZSVP2aMEJOUK0fPhhwcQMrk7C8EiixjsD53xaGX4DSjRH93klf84q1vUfmJ++z\n5uvtP4ESXd4YAde4G+DFTYeQGHA6zUx9c7lB7CPbr
5ZP1cS5YtdnWgY7vdfjzZWQ\nCboWy9oLYEQt8hZ1L0qkyqxT83ryj/0GE39vycXAGTB5fgUTCarl2HEQx1mBWAcN\neZrbw6/Ga
/e7UGSgVX6eV0IzyaQBSdRTqnNDqs0YGce4jqVmYMQnI+ntTtMMLK+N\n1AAphfH++gsCAwEAAaNQME4wHQYDVR0OBBYEFMbCO7AoA1kZvqKN0TV
4vLClBNM1\nMB8GA1UdIwQYMBaAFMbCO7AoA1kZvqKN0TV4vLClBNM1MAwGA1UdEwQFMAMBAf8w\nDQYJKoZIhvcNAQELBQADggIBAHxc4KJiU9k
9bMAqYBX72EsWfFz5SlE8ACnGixSq\nh7Zw8sT97X6URJkiDu8DhoHAA1rKxYZbIeIYSJIJleodltR7Q0LgPyEyBay1GEWX\ndq1CteIFjChtYjA
j/S9xDQP3/M5THQDuH2ATOc7szwWg13u
/8S3l4siA6nPvR6tr\nqYFQK5MrhrLvkAEpJ814qIw4zspT9lrxcALad4M+dUh0UoqF5cFcAaPcRm68N6xN\nfzaDOBSCZWMO2fd7lRvBYK+NREu
2ebuz9wG/ChcKLBuShEaKHkpzPNoEp+sZuiYR\n5q8F6wjA/vFXBaRacSTmRSwHS/fPojVjDgjWlsGKZRYeqvexdiJV0npYdb
/k9x0j\nKk8omjaJT9+yGCliS82/Bszar4vZoonoR5g+XC+
/oDw4tx48dPvW+6hbI7PNbdRI\nasZJTlDfvyavu7dhUm3c90ZiqcpBbDJu1AVtfI5eoQ59WgDUdlTMH2fHY8+q38w3\nAsRVYKB+bNXtfJnt4S6
kWN3DGBhaoubY7oOBLD/IT3NU9CmPHVKV0UwlYpohUyWs\nvOMl8lRlKinOkvpv79C0KYzsN9EwbBsAkS1noxI8Z9m4ySljpfEmqVg1CF7t
/E86\nhr1pq6cgZyrOKVWwNdvaKJ/RTET+HbMY+ytzV9dY+tB7ZA8GFw/yFhuJ386KtsNG\n3imj\n-----END CERTIFICATE-----"
        }
          ],
      "clients": [
        {
          "description": "Example Client",
          "pins": [
            {
              "alg": "sha256",
              "digest": "lLHff44448ne... old pkp...LM4xJe/FaXI/Q5Dcs="
            },
                {
              "alg": "sha256",
              "digest": "lLHff448DjsN... new pkp...lXL21I/A5XlQ02s="
            }
          ],
          "tags": ["exampletag"]
        }
      ]
    }
  ]
}
```


Now publish the metadata to the federation and wait until all entities have downloaded the latest metadata and added the new certificates to their trust repositories. When this is done you should be able to test connection with the new certificate. If it does not work, confirm with the corresponding relying party that they have the correct metadata.

When functionality is confirmed, you can remove the old pins and issuers from your certificate and publish the metadata again. The old certificate is then revoked from the federation.