Manual del integrador del MiniApplet v1.3 del Cliente @firma

este certificado y se continuará con la operación. La línea que debería agregarse a la configuración es, por tanto:

headless=true

Por defecto, si no se establece la propiedad *headless* o se indica un valor distinto de true, se mostrará el diálogo de selección de certificados aun cuando sólo haya un certificado para seleccionar.

Para saber cómo establecer la propiedad *headless* en las operaciones de firma consulte el apartado Paso de parámetros adicionales a los métodos de firma, cofirma y contrafirma.

7.3 Configuración del filtro de certificados

El MiniApplet @firma dispone de filtros de certificados que se pueden aplicar para restringir los certificados que podrá seleccionar el usuario para realizar una operación de firma o multifirma. Los filtros de certificados se pueden establecer como parámetros adicionales en las operaciones de firma, cofirma y contrafirma. Las claves que nos permiten establecer filtros de certificados son:

- *filter*: Esta clave permite establecer uno y sólo uno de los filtros de certificados que se listan más adelante en este apartado. Por ejemplo:
  - *filter*=nonexpired:
    - Certificados no caducados
- *filters*: Esta clave permite establecer uno o más de los filtros de certificados que se listan más adelante en este apartado. Los certificados deberán cumplir las condiciones establecidas en todos los certificados listados, o de lo contrario no se mostrarán. Los distintos filtros se deben separar mediante el carácter punto y coma (';'). Ejemplos:
  - *filters=nonexpired:*
    - Certificados no caducados
  - *filters*=issuer.rfc2254: (O=DIRECCION GENERAL DE LA POLICIA);keyusage.nonrepudiation:true
    - Certificados de firma del DNIe
  - *filters*=issuer.rfc2254: (O=DIRECCION GENERAL DE LA POLICIA);keyusage.nonrepudiation:true;*nonexpired:*
    - Certificados de firma del DNIe no caducados.
- *filters.X*: En esta clave 'X' será un entero igual o mayor que 1. El MiniApplet leerá la clave *filters.1*, a continuación *filters.2* y así hasta que no encuentre una de las claves de la secuencia. Al contrario que con la clave *filters*, basta con que el certificado cumpla uno de estos filtros para que se muestre. No es necesario cumplirlos todos. Cada uno de estas

claves puede declarar varios filtros separados por punto y coma (';') de tal forma que sí se deberán cumplir todos ellos para satisfacer ese subfiltro concreto. Ejemplo:

- *filters.1*=issuer.rfc2254:(O=DIRECCION GENERAL DE LA POLICIA);keyusage.nonrepudiation:true
- *filters.2*=issuer.rfc2254:(O=FNMT)
    - La conjunción de estas dos claves en una operación de firma hará que sólo se muestren al usuario los certificados CERES y el de firma del DNIe.

Estas tres claves de definición de filtros son excluyentes y tienen la prioridad según la que se listan (*filter*, *filters* y *filters.X*). Es decir, si se establece la propiedad filter, no se procesarán las propiedades *filters* y *filters.1*, por ejemplo.

Los filtros disponibles en el MiniApplet son:

- Filtro DNIe: Filtra los certificados del almacén para que sólo se muestren los certificados de firma de los DNIe disponibles desde ese almacén.
    - Para establecer este filtro de certificados se indicará la propiedad *filter* con el valor *dnie:* en el parámetro de configuración de la operación de firma, cofirma o contrafirma.
    - Ejemplo:
        - `filter=dnie:`
- Filtro de certificados de firma: Filtra los certificados del almacén para que no se muestren los considerados certificados de autenticación. Esta exclusión no se realiza mediante KeyUsage para evitar que queden excluidos certificados mal identificados. Un ejemplo de certificado que no se mostrará en el diálogo es el de autenticación del DNIe.
    - Para establecer este filtro de certificados se indicará la propiedad *filter* con el valor *signingCert:* en el parámetro de configuración de la operación de firma, cofirma o contrafirma.
    - Ejemplo:
        - `filter=signingCert:`
- Filtro de certificados de autenticación: Filtra los certificados del almacén para que no se muestren los específicos para firma avanzada reconocida. Esta exclusión no se realiza mediante KeyUsage para evitar que queden excluidos certificados mal identificados. Un ejemplo de certificado que no se mostrará en el diálogo es el de firma del DNIe.
    - Para establecer este filtro de certificados se indicará la propiedad *filter* con el valor *authCert:* en el parámetro de configuración de la operación de firma, cofirma o contrafirma.
    - Ejemplo:
        - `filter=authCert:`

- Filtro de certificados SSCD: Filtra los certificados del almacén para que se muestren sólo aquellos emitidos por medio de un dispositivo SSCD (dispositivo seguro de creación de firma), como es el caso de los certificados del DNIe. Hay que tener en cuenta que el filtrado se realiza a partir de un atributo QCStatement declarado en el propio certificado. Si la autoridad de certificación no incluye este atributo, no será posible realizar la distinción.
    - Para establecer este filtro de certificados se indicará la propiedad *filter* con el valor *sscd:* en el parámetro de configuración de la operación de firma, cofirma o contrafirma.
    - Ejemplo:
        - `filter=sscd:`
- Filtro SSL: Filtra los certificados del almacén para que sólo se muestre aquellos con un número de serie concreto (comúnmente sólo será uno). Existe un caso especial. Si el número de serie resulta ser de un certificado de autenticación de un DNIe, se mostrará en su lugar el certificado de firma de ese mismo DNIe.
    - Para establecer este filtro de certificados se indicará la propiedad *filter* con el valor *ssl:*, seguido por el número de serie del certificado, en el parámetro de configuración de la operación de firma, cofirma o contrafirma. Esto es: *filter=ssl:Nº_serie*. El número de serie se debe indicar en hexadecimal:
    - Ejemplos:
        - `filter=ssl:45553a61`
        - `filter=ssl:03ea`
- Filtro de certificados cualificados de firma: Filtra los certificados del almacén para que sólo se muestre aquellos con un número de serie concreto (comúnmente sólo será uno). En el caso de que este certificado no esté cualificado para firma, se buscará un certificado parejo que sí lo esté en el almacén. Si se encontrase se seleccionaría este nuevo certificado y, si no, se seleccionará el certificado al que corresponde el número de serie.
    - Para establecer este filtro de certificados se indicará la propiedad *filter* con el valor *qualified:*, seguido por el número de serie del certificado, en el parámetro de configuración de la operación de firma, cofirma o contrafirma. Esto es: *filter=qualified:Nº_serie*. El número de serie se debe indicar en hexadecimal:
    - Ejemplos:
        - `filter=qualified:45553a61`
        - `filter=qualified:03ea`
- Filtro de certificados caducados: Filtra aquellos certificados que se encuentran fuera de su periodo de validez para que sólo se muestren los certificados vigentes, que son los únicos que pueden generar una firma válida.
    - Para establecer este filtro se usará la palabra clave *nonexpired:*
    - Ejemplo:
        - `filter=nonexpired:`

- Filtro por huella digital (Thumbprint): Filtra los certificados de tal forma que sólo se mostrará aquel que tenga la huella digital indicada. Hay que tener en cuenta que esta huella digital no debe calcularse en base a un fichero (por ejemplo, un ".cer"), sino que es la huella digital de la codificación del certificado.
    - Para establecer este filtro se usará la palabra clave *thumbprint:*, seguida del algoritmo de huella digital utilizado y, separado por el carácter dos puntos (':') la huella digital que se busque en hexadecimal.
    - Ejemplo:
        - `filter=thumbprint:SHA1:30 3a bb 15 44 3a fd d7 c5 a2 52 dc a5 54 f4 c5 ee 8a a5 4d`
            - Este filtro sólo mostrará el certificado cuya huella digital en SHA1 sea la indicada.
- Filtro RFC2254 en base al *Subject* del certificado: Filtra los certificados a partir de una expresión regular creada según la RFC2254 que se aplica sobre el *Subject* del certificado.
    - Para establecer este filtro se usará el valor *subject.rfc2254:* seguido de la expresión RFC2254.
    - Puede revisarse la normativa RFC 2254 en http://www.faqs.org/rfcs/rfc2254.html
    - Ejemplo:
        - `filter=subject.rfc2254:(CN=*12345678z*)`
            - Este filtro mostrará sólo aquellos certificados en los que aparezca la cadena "12345678z" en el *CommonName* de su *Subject*.
- Filtro RFC2254 en base al *Issuer* del certificado: Filtra los certificados a partir de una expresión regular creada según la RFC2254 que se aplica sobre el *Issuer* del certificado.
    - Para establecer este filtro se usará el valor *issuer.rfc2254:* seguido de la expresión RFC2254.
    - Puede revisarse la normativa RFC 2254 en http://www.faqs.org/rfcs/rfc2254.html
    - Ejemplo:
        - `filter=issuer.rfc2254:(|(O=FNMT)(O=DIRECCION GENERAL DE LA POLICIA))`
            - Este filtro mostrará sólo aquellos certificados cuyo *Issuer* tenga establecido como organización "FNMT" o "DIRECCION GENERAL DE LA POLICIA", es decir, sólo mostrará los certificados del DNIe y los de CERES.
- Filtro de texto en base al *Subject* del certificado: Filtra los certificados según si contienen o no una cadena de texto en el *Principal* de su *Subject*.
    - Para establecer este filtro se usará el valor *subject.contains:* seguido de la cadena de texto que debe contener.
    - Ejemplo:
        - `filter=subject.contains:JUAN ESPAÑOL ESPAÑOL`

- Este filtro mostrará sólo aquellos certificados en los que aparezca la cadena "JUAN ESPAÑOL ESPAÑOL" en el *Subject*.

- Filtro de texto en base al *Issuer* del certificado: Filtra los certificados según si contienen o no una cadena de texto en el *Principal* de su *Issuer*.
  - Para establecer este filtro se usará el valor *issuer.contains:* seguido de la cadena de texto que debe contener.
  - Ejemplo:
    - `filter=issuer.contains:O=EMPRESA`
      - Este filtro mostrará sólo aquellos certificados en los que el *Principal* del *Issuer* muestre el texto "O=EMPRESA".
- Filtros por uso declarado de los certificados (*KeyUsage*): Colección de filtros que permiten filtrar según el uso declarado de los certificados.
  - Para establecer estos filtros usaremos las siguientes claves según los usos que se quieran comprobar. Las claves irán seguidas de los valores "true" o "false", según se desee que el uso esté habilitado o no lo esté, respectivamente:
    - *keyusage.digitalsignature:*
    - *keyusage.nonrepudiation:*
    - *keyusage.keyencipherment:*
    - *keyusage.dataencipherment:*
    - *keyusage.keyagreement:*
    - *keyusage.keycertsign:*
    - *keyusage.crlsign:*
    - *keyusage.encipheronly:*
    - *keyusage.decipheronly:*
  - Los *KeyUsages* que no se declaren en el filtro no se tendrán en cuenta.
  - Ejemplos:
    - `filters=keyusage.digitalsignature:true;keyusage.keyencipherment:true`
      - Este filtro mostrará sólo aquellos certificados que tengan establecidos a `true` los *KeyUsage* `digitalsignature` (autenticación) y `keyencipherment` (sobres electrónicos), ignorando el valor del resto de *KeyUsages*. Este filtro mostrará, por ejemplo, los certificados de la FNMT.
    - `filters=keyusage.nonrepudiation:true`
      - Este filtro mostrará sólo aquellos certificados que tengan establecidos a `true` el `nonrepudiation` (firma avanzada). Este filtro mostrará, por ejemplo, el certificado de firma del DNIe.

Se ignorará cualquier valor establecido como filtro de certificados distinto a los que se han listado.

Si ningún certificado cumple los criterios de filtrado, se lanzará una excepción indicando que no se ha encontrado ningún certificado que cumpla con los criterios indicados y se cancelará la operación.

Si más de un certificado cumple los criterios de filtrado, se mostrarán todos ellos en el diálogo de selección de certificados.

Si tan sólo un certificado cumple con las condiciones de los filtros establecidos y se ha configurado la opción *headless* en las propiedades adicionales de la operación, se seleccionará automáticamente ese certificado sin mostrar el diálogo de selección al usuario. Consulte el apartado Selección automática de certificados para conocer cómo configurar la propiedad *headless*.

Para saber cómo establecer la configuración de los filtros de certificados en las operaciones de firma consulte el apartado Paso de parámetros adicionales a los métodos de firma, cofirma y contrafirma.

7.4 Configuración de la política de firma

7.4.1 Configuración manual

La política de firma de una firma electrónica identifica diversos criterios que se han cumplido durante la construcción de esta firma o requisitos que cumple la propia firma. Esta política de una firma electrónica se identifica mediante varios atributos declarados en la firma. Todos los formatos avanzados de firma (CAdES y XAdES) tienen una variante EPES (*Explicit Poliyc-based Electronic Signature*) que declaran los atributos correspondientes a la política de firma.

El MiniApplet @firma permite la generación de firmas EPES (CAdES-EPES y XAdES-EPES) para lo cual es necesario indicar las propiedades de la política en el método de firma que se vaya a utilizar.

Consulte el apartado específico de configuración del formato de firma que desee utilizar para conocer las propiedades disponibles para la configuración de la política de firma.

Para saber cómo establecer estas las propiedades de firma, consulte el apartado Paso de parámetros adicionales a los métodos de firma, cofirma y contrafirma.

Tenga en cuenta que el que una firma incluya los atributos correspondientes a una política de firma concreta no significa que cumpla los criterios de la política. Si desea que sus firmas se ajusten a una política de firma lea las restricciones impuestas por esa política y genere firmas acorde a ella antes de configurarla. De esta forma, podrá asegurarse de que sus firmas son compatibles con otros sistemas y entornos en los que se utilicen firmas acorde a la política en cuestión.

7.4.2 Política de firma de la AGE v1.9

En el MiniApplet @firma se ha incluido un mecanismo para la configuración rápida y sencilla de la política de firma de la Administración General del Estado (AGE) v1.9. Para configurar esta política