Migration SHA-2

SHA-1 ➔ SHA-2

- SHA1, SHA-2, …
  - algorithmes de calcul d´empreinte pour la signature des certificats

SHA-1 ➔ SHA-2

- Certificats GRID2-FR utilise SHA1

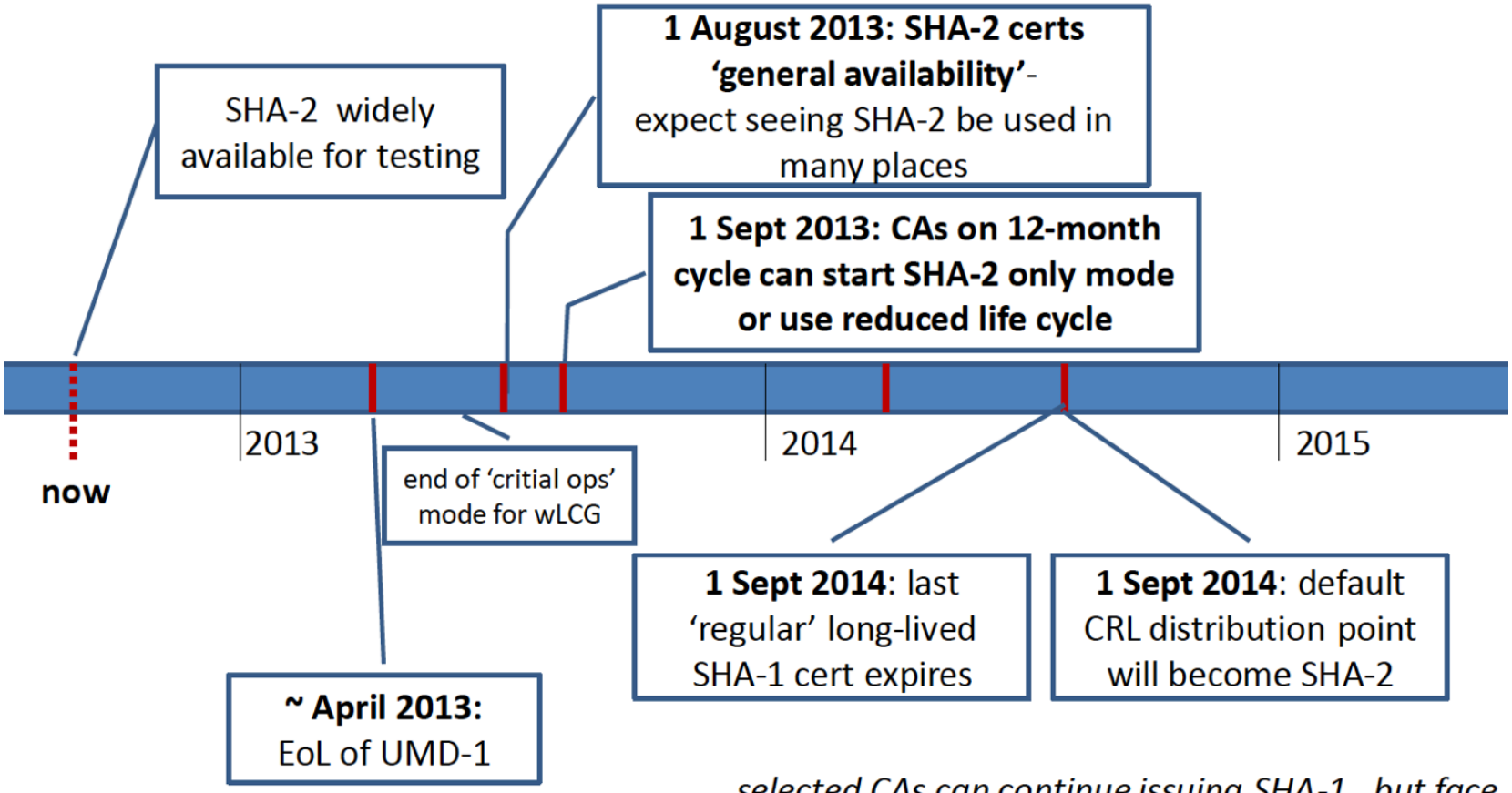
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7246 (0x1c4e)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, O=CNRS, CN=GRID2-FR
        Validity
            Not Before: Aug  8 14:36:26 2012 GMT
            Not After : Sep  5 14:36:26 2012 GMT
        Subject: O=GRID-FR, C=FR, O=RENATER, OU=SSI, CN=Claude Gross
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:af:4d:37:26:85:1d:f0:4d:1f:32:a9:2d:a2:51:
                                    ……….
                    33:dc:67:81:28:8c:2f:ae:7a:1a:21:b1:86:79:e5:
                    b1:71
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            …….
Signature Algorithm: sha1WithRSAEncryption
        77:4d:44:d3:0f:82:91:ab:30:05:7a:2c:42:7c:72:21:df:b0:
        ……
```

SHA-1 ➔ SHA-2

- Depuis 2009, SHA-1 est considéré comme moins fiable

➜ Plan de migration vers SHA-2

Planning



selected CAs can continue issuing SHA-1 , but face risk of removal in case SHA-1 is broken

Planning

- Au 01 Octobre 2012 : Chaque AC doit être capable de générer des certificats SHA-2 en local pour les tests.
- Au 01 Août 2013 : Début d'émission des certificats signés SHA-2 par les ACs membre de IGTF, en notant que ces ACs ne sont pas autorisées à émettre des certificats signés SHA-2 avant cette date.
  Cela ne signifie pas que tous les certificats qui seront émis après 01 Août 2013 devront être en SHA-2.
- Au 01 Septembre 2013 : délivrance des certificats SHA-2 seulement avec la possibilité de délivrer de certificats SHA-1 avec une date d'expiration correspond au 01 Septembre 2014.
- Au 01 Septembre 2014 : Tous les certificats émis doivent être signés SHA-2 , et les derniers certificats SHA-1 seront expirés (fin de vie des certificats SHA-1).
  Si il se trouve des certificats SHA-1 valide après cette date, alors le risque sera le retrait de ladite CA de l'IGTF, et de l'EGI.

Tests

http://igc.services.cnrs.fr/GRID-FR-SHA2/