RA - Download Pseudonym Certificate Batch

OBEs use this service to download a batch of Pseudonym Certificates for a specific time period.

PORT	8892
PATH	/download/batch
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Download-Req' containing a Base64 encoded ASN.1 serialized *SecuredAuthenticatedDownloadRequest,* containing a *SignedAuthenticatedDownloadRequest,* containing a *ScopedAuthenticatedDownloadRequest*, containing an *AuthenticatedDownloadRequest* with a *filename* property of the form [0-9A-F]{16}_[0-9A-F]{1,8}.zip, where the first group of 16 hexadecimal digits is the device's request hash obtained from the initial provision pseudonym certificate batch request, and the second group of up to 8 hexadecimal digits is the i-value. Example: AB09281C9867DE53_F.zip corresponds to i value 15, for device with request hash AB09281C9867DE53. **Range (optional) as defined in RFC 2616:** To support partial downloads for resuming interrupted transfers. Examples: 1. From byte offset 500 to 700: Range : bytes=500-700 2. Starting from byte offset 1000 to the end: Range : bytes=1000-
HTTP Response Body	If no Range header is present, the entire zip file corresponding to the requested batch. If a Range header is present, the specified bytes of the referenced file.

Preconditions

1. The requested batch has already been generated
2. The requesting device has not been previously revoked

Postconditions

1. The zip file corresponding to the batch specification in the request URL is returned.
2. The content of the zip file is organized as a flat directory containing *n* files (where 0 <= *n* <= *j_max* - 1) with the naming format:
   a. X_Y (NOTE: no file extension)
   b. Where X is the i-value representing the SCMS I period in which the certificate is valid in hexadecimal
   c. Where Y is a sequence of "j" values from j = 0 to j = j_max-1 in hexadecimal
   d. Example zip file contents for period i=55, j = 20:
      i. 37_0
      ii. 37_1
      iii. ...
      iv. 37_12
      v. 37_13
   e. The contents of each individual file within the .zip is a binary OER encoding of the appropriate SignedEncryptedCertificateResponse.

Error Handling

See "RA-EE Errors" in Overview of Used Error Codes

Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The number of files downloaded in a year is a function of the number of years in service:

$$f(year) = \left(\sum_{i=1}^{year-1} (17million \times 52weeks) \right) + (17million \times 156weeks)$$

which assumes 17 million vehicles are added each year.

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Throughput	Assuming 17 million new vehicles downloading the initial three years' worth of certificates (156 files) plus old cars downloading one year's worth of certificates (52 files).	With no previous year vehicles: 17m x 52 weeks * 3 years = 2,652 million files Divided by the number of seconds in a year: 2,652 million files / 31,557,600 seconds = **85 files per second**	With and two years' worth of old vehicles (34 million): 17m (new) + 34m (old) Old cars only download one year's worth of certificates (52 files) while new cars download three years' worth of certificates (156 files) so: (17m * 156 files) + (34m * 52 files) = 2,652 million files + 1,768 million files = 4,420 million files Divided by the number of seconds in a year: 4,420 million files /31,557,600 seconds = **~141 files per second**	With four years' worth of old vehicles (68 million): 17m (new) + 68m (old) Old cars only download one year's worth of certificates (52 files) while new cars download three years' worth of certificates (156 files) so: (17m * 156 files) + (68m * 52 files) = 2,652 million files + 3,536 million files = 6,188 million files Divided by the number of seconds in a year: 6,188 million files /31,557,600 seconds = **~197 files per second**	At the end of the first 10 years, there will be a total of 170 million cars in the system out of which, 153 million will be old vehicles: 17m (new) + 153m (old) The new cars will be downloading three years' worth of certificates (156 weeks), while the rest of the vehicles will be topping up only (52 weeks). Since each file contains one week's worth of certificates, we can express this in number of files: (17m x 156 files) + (153m x 52 files) = (2,652 mf + 7,956mf) = 10,608 million files Divided by the number of seconds in a year: 15,028 million files / 31,557,600 seconds = **~337 files per second**

Quality of Protection

- RA protects access with HTTPS (TLS V1.2)
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
- Uses certificate-based client authentication of data signed by the device enrollment certificate, validated at the application layer. This is a supplement to the one-way TLS authentication, to provide two-way authentication with a TLS/1609.2 hybrid scheme.