Maintaining the root certificates

Node.js contains a compiled-in set of root certificates used as trust anchors for TLS certificate validation.

The certificates come from Mozilla, specifically NSS's `certdata.txt` file.

The PEM encodings of the certificates are converted to C strings, and committed in `src/node_root_certs.h`.

When to update

Root certificates should be updated sometime after Mozilla makes an NSS release, check the NSS release schedule.

Process

Commands assume that the current working directory is the root of a checkout of the nodejs/node repository.

1. Find NSS metadata for update.

   The latest released NSS version, release date, Firefox version, and Firefox release date can be found in the NSS release schedule.

   The tag to fetch `certdata.txt` from is found by looking for the release version in the tag list.

2. Update `certdata.txt` from the NSS release tag.

   Update the tag in the commands below, and run:

   ```
   cd tools/
   ./mk-ca-bundle.pl -v 2>_before
   curl -O https://hg.mozilla.org/projects/nss/raw-
   file/NSS_3_41_RTM/lib/ckfw/builtins/certdata.txt
   ```

   The `_before` file will be used later. Verify that running `mk-ca-bundle` made no changes to `src/node_root_certs.h`. If it did, something went wrong with the previous update. Seek help!

   Update metadata in the message below, and commit `certdata.txt`:

   ```
   tools: update certdata.txt

   This is the certdata.txt[0] from NSS 3.41, released on 2018-12-03.

   This is the version of NSS that will ship in Firefox 65 on
   2018-12-11.

   [0] https://hg.mozilla.org/projects/nss/raw-
   file/NSS_3_41_RTM/lib/ckfw/builtins/certdata.txt
   ```

3. Update `node_root_certs.h` from `certdata.txt`.

   Run the command below:

   ```
   ./mk-ca-bundle.pl -v 2>_after
   ```

Confirm that `../src/node_root_certs.h` was updated.

Determine what changes were made by diffing the before and after files:

```
% diff _before _after
11d10
< Parsing: Visa eCommerce Root
106d104
< Parsing: TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5
113,117d110
< Parsing: Certplus Root CA G1
< Parsing: Certplus Root CA G2
< Parsing: OpenTrust Root CA G1
< Parsing: OpenTrust Root CA G2
< Parsing: OpenTrust Root CA G3
134c127,136
< Done (133 CA certs processed, 20 skipped).
---
> Parsing: GlobalSign Root CA - R6
> Parsing: OISTE WISeKey Global Root GC CA
> Parsing: GTS Root R1
> Parsing: GTS Root R2
> Parsing: GTS Root R3
> Parsing: GTS Root R4
> Parsing: UCA Global G2 Root
> Parsing: UCA Extended Validation Root
> Parsing: Certigna Root CA
> Done (135 CA certs processed, 16 skipped).
```

Use the diff to update the message below, and commit `src/node_root_certs.h`:

```
crypto: update root certificates

Update the list of root certificates in src/node_root_certs.h with
tools/mk-ca-bundle.pl.

Certificates added:
- GlobalSign Root CA - R6
- OISTE WISeKey Global Root GC CA
- GTS Root R1
- GTS Root R2
- GTS Root R3
- GTS Root R4
- UCA Global G2 Root
- UCA Extended Validation Root
- Certigna Root CA

Certificates removed:
- Visa eCommerce Root
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5
```

```
- Certplus Root CA G1
- Certplus Root CA G2
- OpenTrust Root CA G1
- OpenTrust Root CA G2
- OpenTrust Root CA G3
```