Behind The Padlock

Tale of Slip-up & Certificate's

Presented By

Tanishq Solanki Malav Patel

Agenda

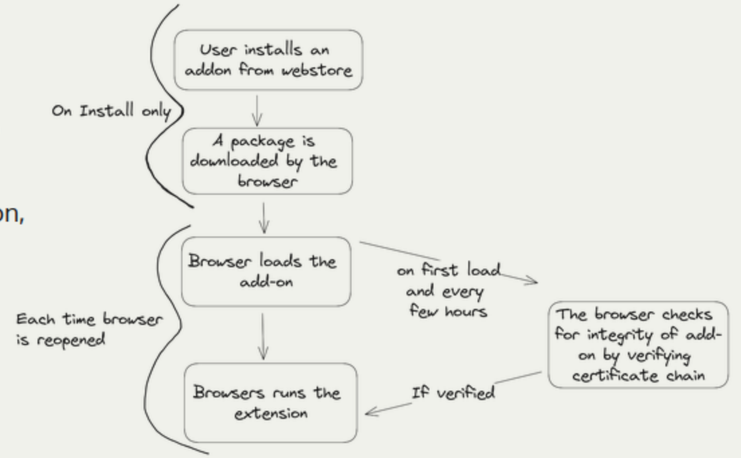
- Man in the Middle Attack
- Public Key* Encryption 101
- Certificates 101
- Why Trust CA ?
- Add-ons 101
- Resolution to the Slip-up
- Summary

Tale of Firefox Add-on Slip-up

- On 2019 Star-wars day i.e. May 4th, 2019, Firefox started receiving many many reports.
- The browser became suddenly unusable for some individuals at random times.
- It was crashing for some while others had to deal with minor inconveniences.
- More than half of the users were affected by this phenomenon.
- Firefox team went all-out to find the cause.
- It was found that the add-on signing processes "Intermediary certificate" expired.
- Tech team began to brainstorm a solution.
- A fix was deployed within 12 hrs from the incident.

Add-ons 101

- Add-on are in-essence apps for browser.
- They are made in web languages and are permitted to use Extensions only API's.
- They can modify HTML, CSS and add Js to be used on webpage or listen events.
- It can add features like QR code generation, ChatGPT prompt to each webpage, password managers.
- Usually installed from a browser specific appstore.
- The extensions are reviewed by staff at appstore for its listed purposes and permissions used that are declared in a manifest.
- Eg. Grammerly, Ad-Blockers, Text-to-Speech.



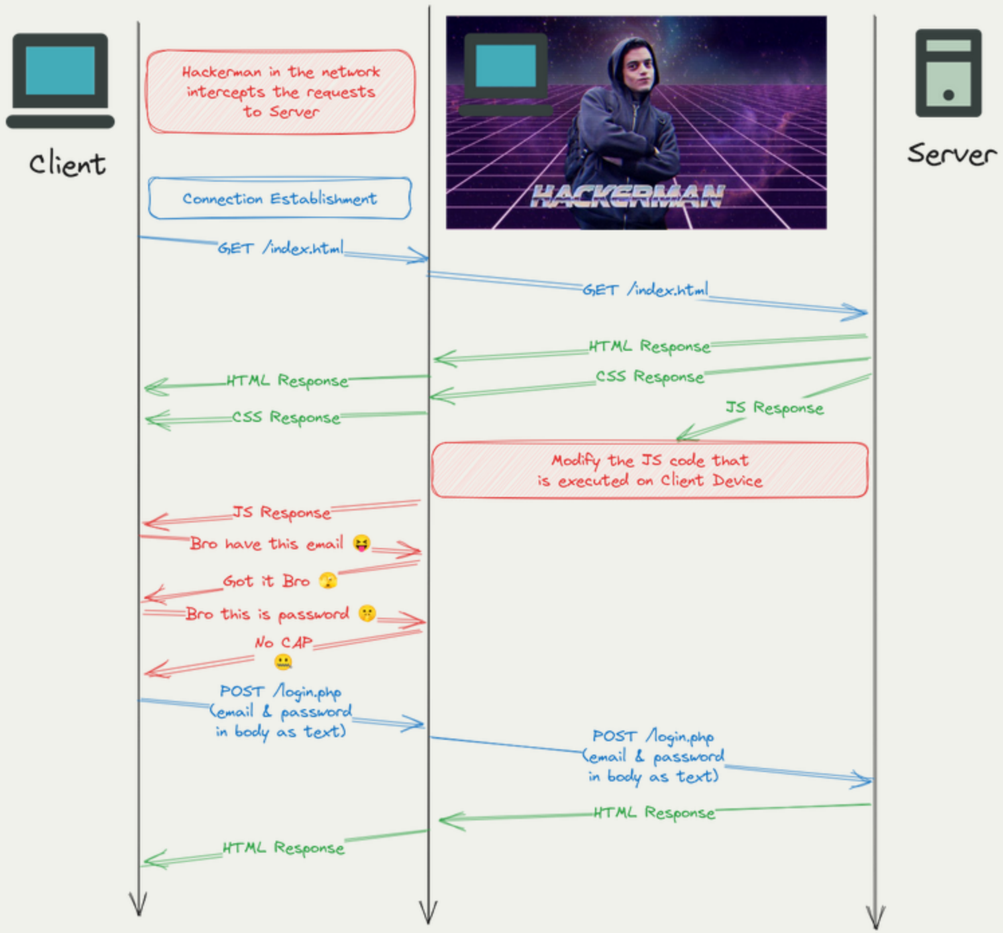
why this is necessary?

"Hacker"

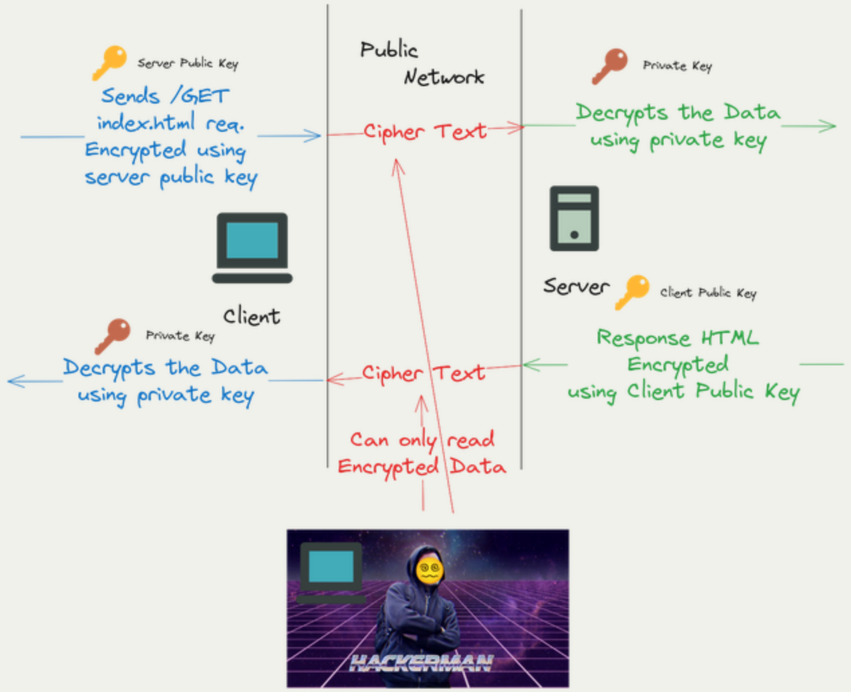
Man in the Middle Attack

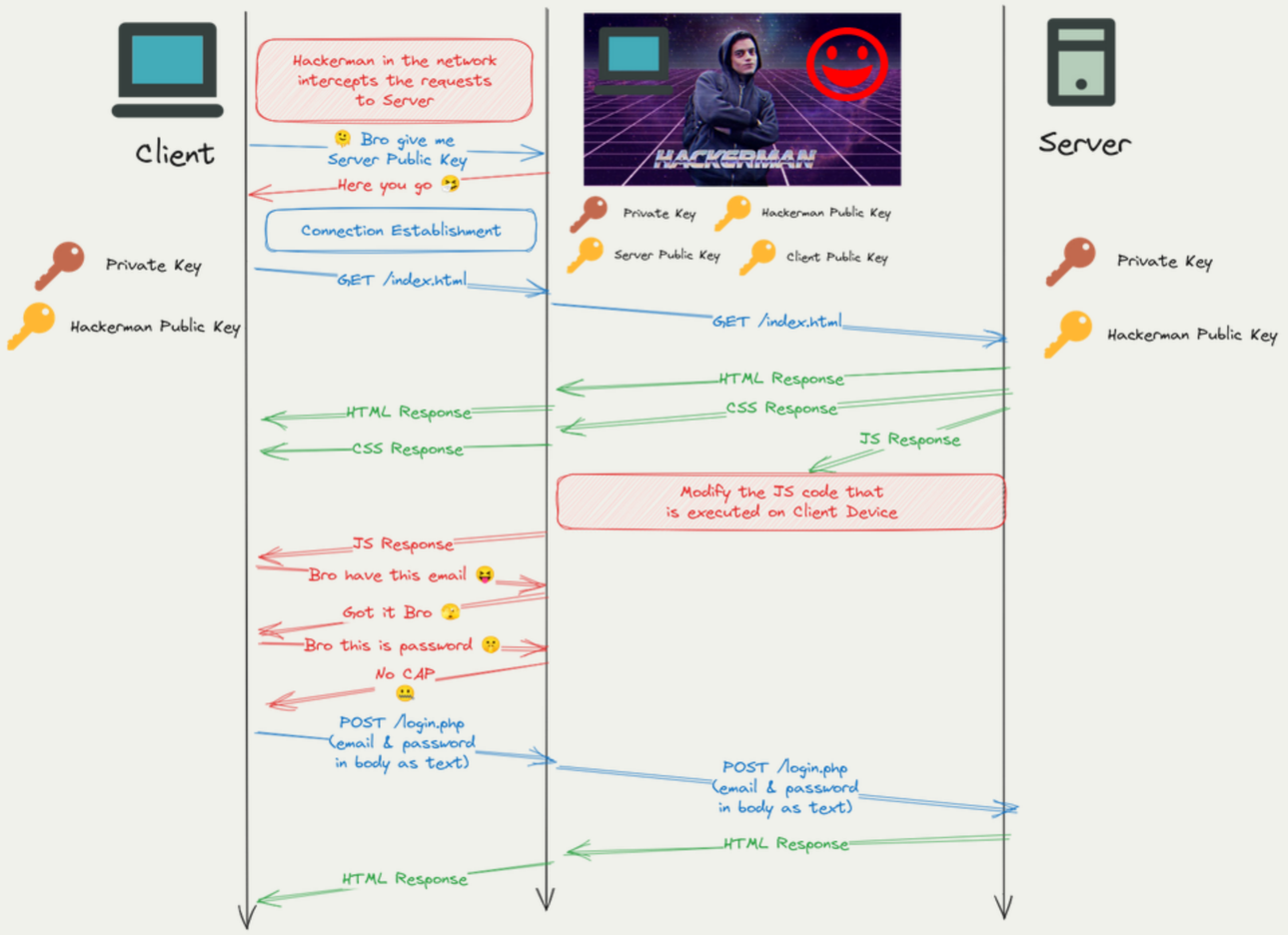
This Meme falls under Fair Use

- An attack that can be executed in "any kind" of Network.
- A Third and Unauthorized Party Inserts themselves between the two parties involved in a certain endeavor.
- A non-computer science related example – plot of a certain Bollywood movie "Hera Pheri".


Client
Hackerman in the network intercepts the requests to Server
HACKERMAN
Server
Connection Establishment
GET /index.html
GET /index.html
HTML Response
HTML Response
CSS Response
CSS Response
JS Response
Modify the JS code that is executed on Client Device
JS Response
Bro have this email 😝
Got it Bro 🤔
Bro this is password 🤫
No CAP 😬
POST /login.php (email & password in body as text)
POST /login.php (email & password in body as text)
HTML Response
HTML Response

Public Key Encryption* 101




Client
Server
Hackerman in the network intercepts the requests to Server
Bro give me Server Public Key
Here you go
Connection Establishment
Private Key
Hackerman Public Key
GET /index.html
GET /index.html
HTML Response
CSS Response
HTML Response
CSS Response
JS Response
Modify the JS code that is executed on Client Device
JS Response
Bro have this email
Got it Bro
Bro this is password
No CAP
POST /login.php (email & password in body as text)
POST /login.php (email & password in body as text)
HTML Response
HTML Response
Private Key
Hackerman Public Key
Server Public Key
Client Public Key
Private Key
Hackerman Public Key

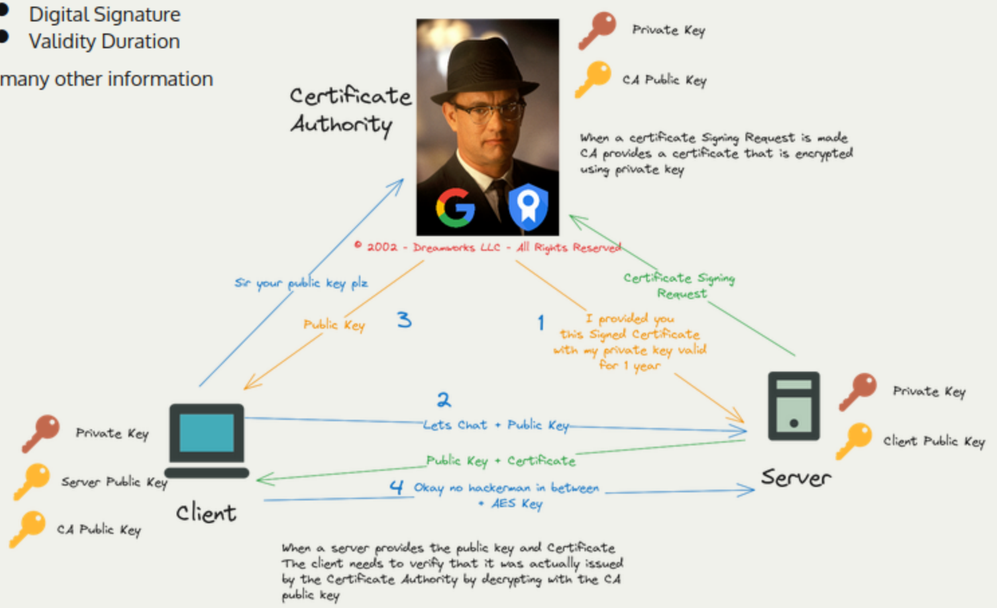
Certificate 101

Include

- Subject Name
- Public Key (Subject)
- Issuer Name
- Digital Signature
- Validity Duration

and many other information

- Key exchange without certificates lacks authentication and can be vulnerable to man-in-the-middle attacks.
- Certificates provide a trusted third-party verification of identity, ensuring secure communication.



Why Trust CA?

Certificate Chain

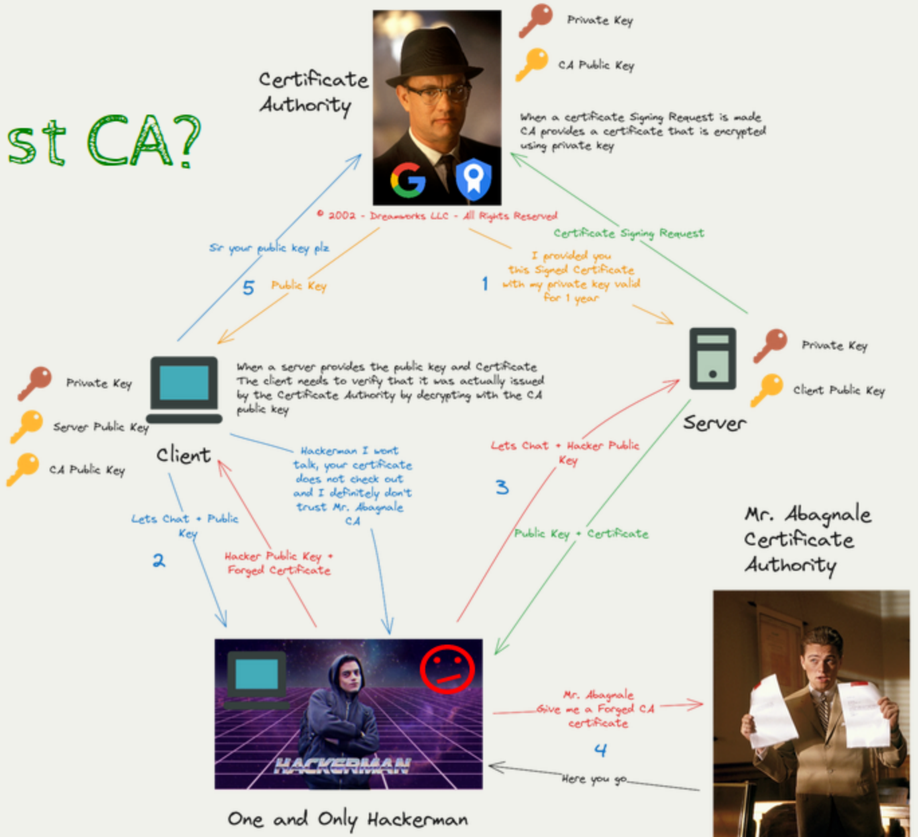
Subject: myprotfolio.dev
Issuer: Google Trusted LLC CA

Client Verifies the Certificate chain

Subject: Google Trusted LLC CA
Issuer: Google Root CA

Until a root CA is reached where certificate is installed user machine

Subject: Google Root CA
Issuer: Google Root CA

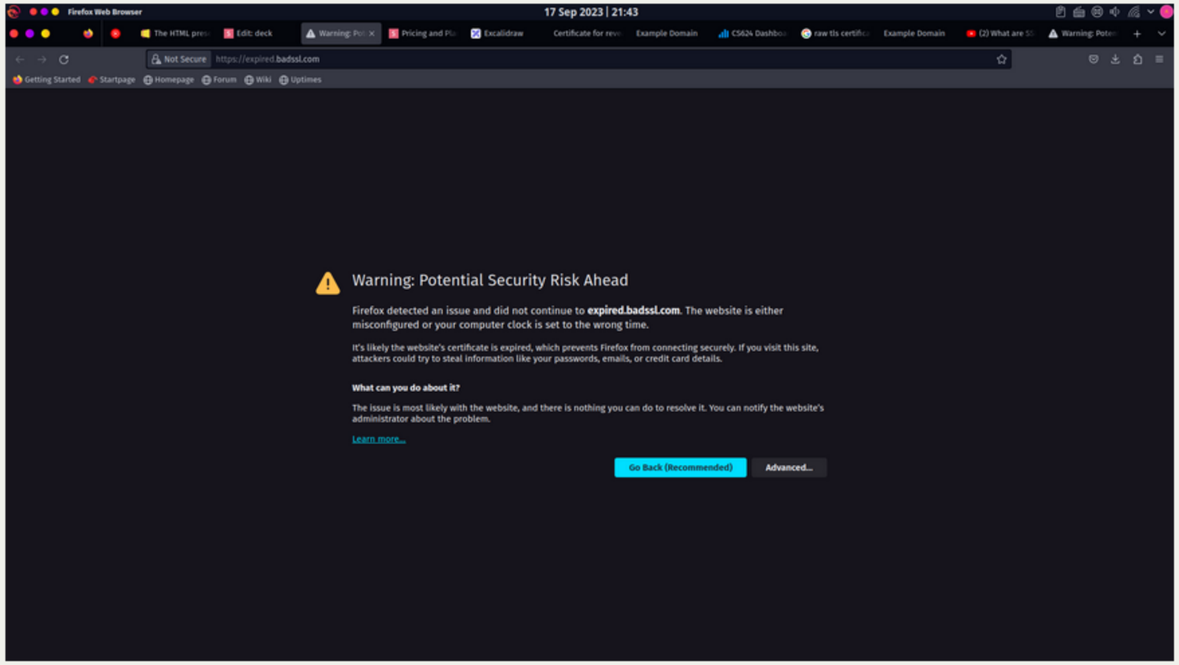


Credit: Andrew Cooper
In the movie "Catch Me If You Can," Leonardo DiCaprio plays Frank Abagnale.

Expired Certificate

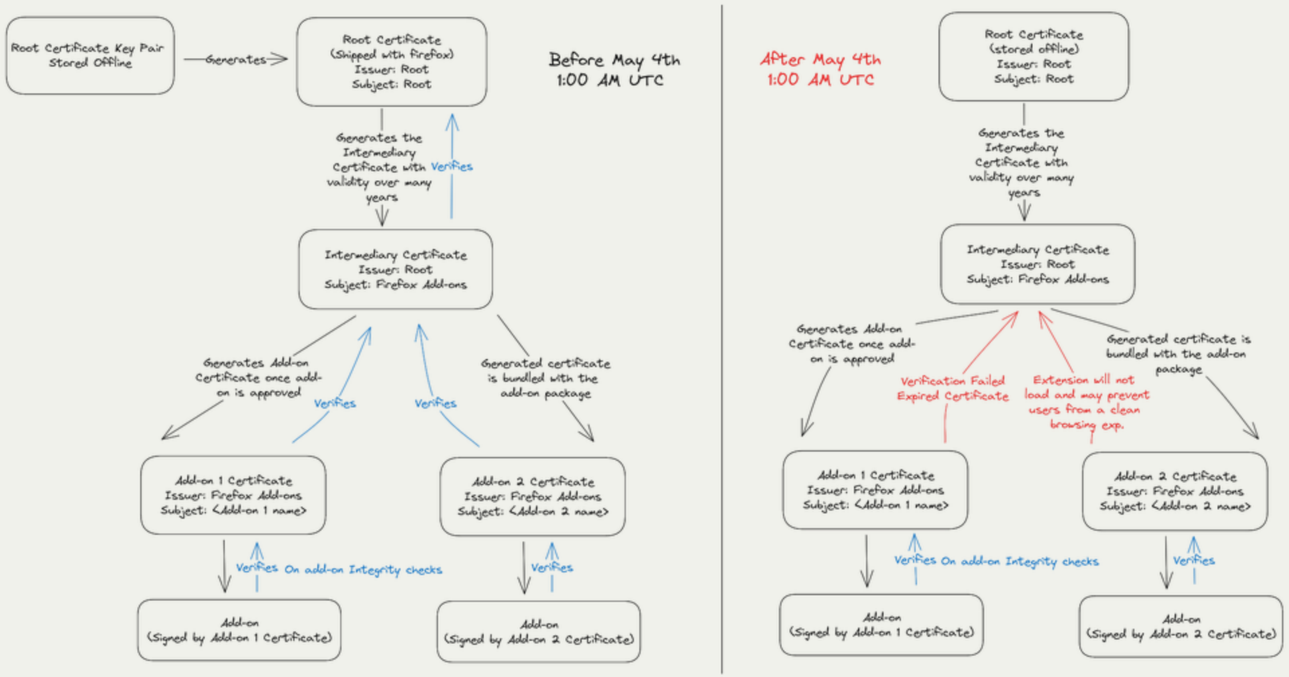
Link to one - Website with Expired Certificate

Link to - website where you can explore various other errors of bad ssl certificates



Firefox

Add-on Signing Process & Integrity Check



Hotfix - Disable Add-on Verification

The Integrity check process is done randomly for users so not all the users were affected in the window spanning the incident report time to hotfix update.

To have the unaffected users not face this issue Tech. team released a major version of Firefox built with disabled Integrity checks so they wont experience any inconveniences

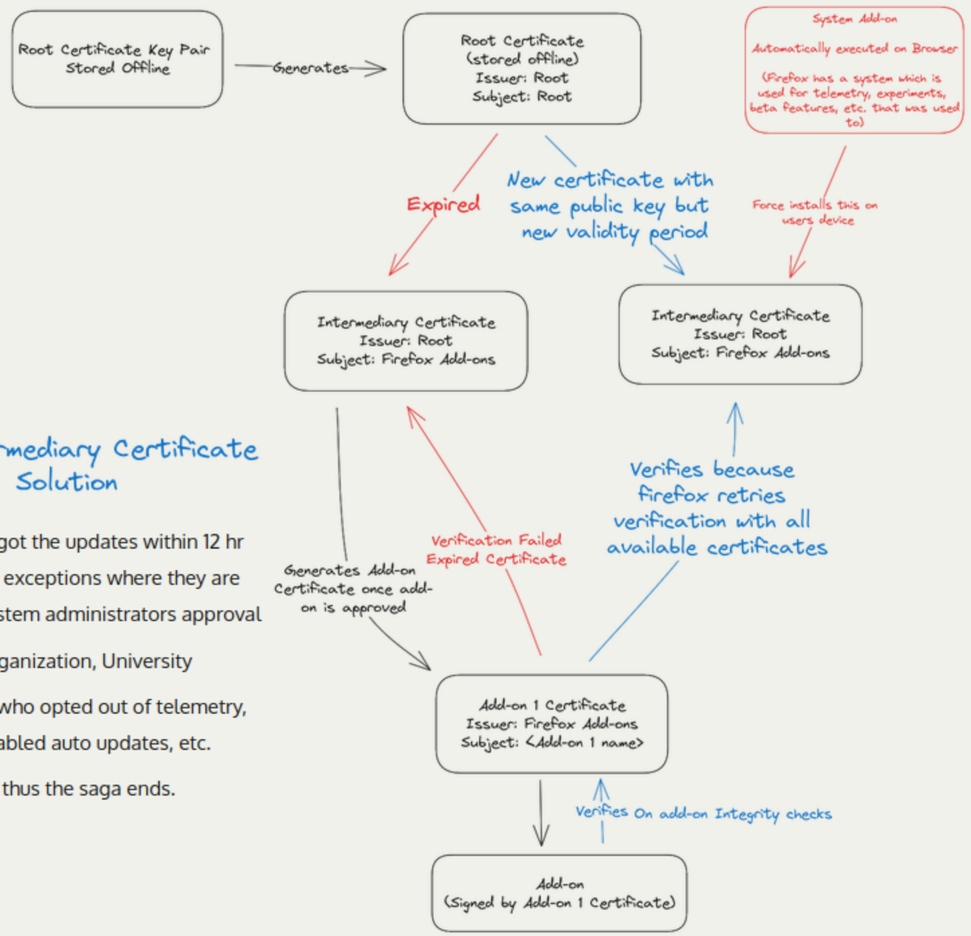
Solution - Install New Intermediary Certificate

As for a proper solution to solve the issue team pursued 2 ideas.

1 - Have the Firefox add-on verification done using a back dated time (Time Travel) so the add-on integrity check still works.

2 - Create a new Certificate with root key pair and have it Installed on Firefox remotely and force the browser to re-validate the integrity.

Eventually Tech. team ended up pursuing 2'nd idea.



New Intermediary Certificate Solution

Most users got the updates within 12 hr period with exceptions where they are behind the system administrators approval

i.e. Organization, University

and people who opted out of telemetry, who disabled auto updates, etc.

And thus the saga ends.

Lessons

- Have a Big Red Fail button ready to be pushed.
- "Plan" - have reminders, calendar events.
- Have a robust system that can help push updates to user.
- Track everything in a large enough projects.
- Software is never always reliable.

Thank you & Questions?