Government Domains and SSL Policy Oversight.

In order to improve efficiency, most countries employ so-called E-Services. They expedite a lot of work for citizens. However, processing sensitive data seems not to be secure enough.

The research will cover an example of Republic of Serbia.

The specific case will cover two government websites including:

- E-uprava (https://www.euprava.gov.rs/)
- National Bank Of Serbia (https://www.nbs.rs)

Those services are used for:

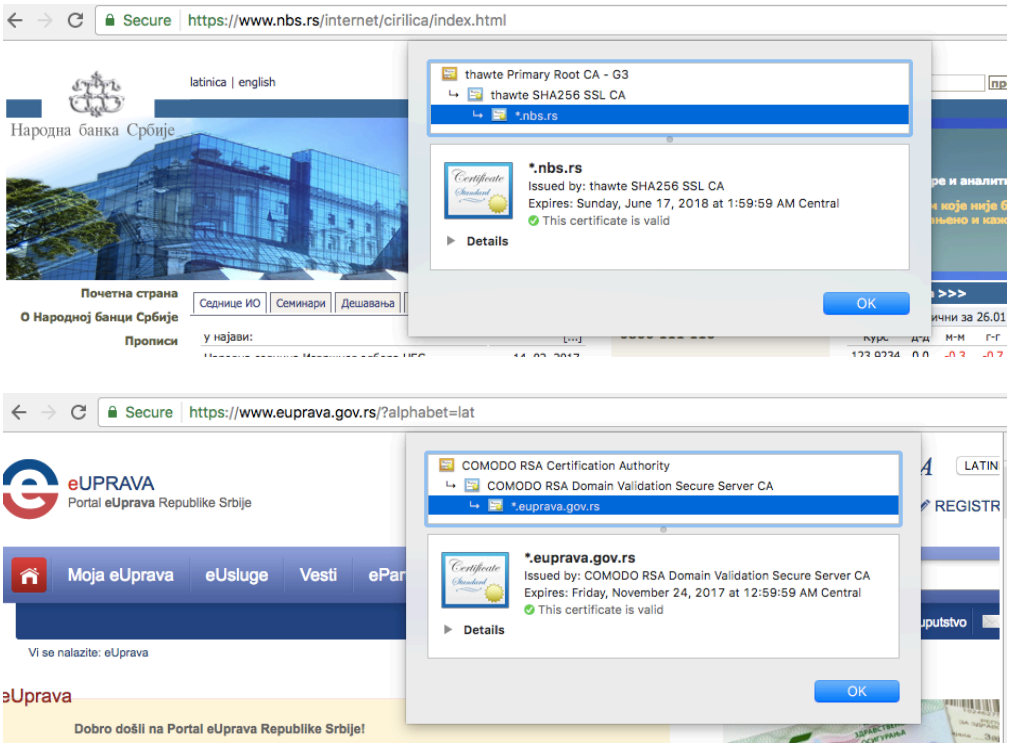
- Filling Tax Reports.
- Submitting requests for government documents such as passport renewal.
- Signing up children into a kindergarten.
- A lot more services, even those that requires smart card reader and transmission of Personal ID public key.

The services in questions are secured by SSL issued by Comodo, and Thawte.

The main problem:

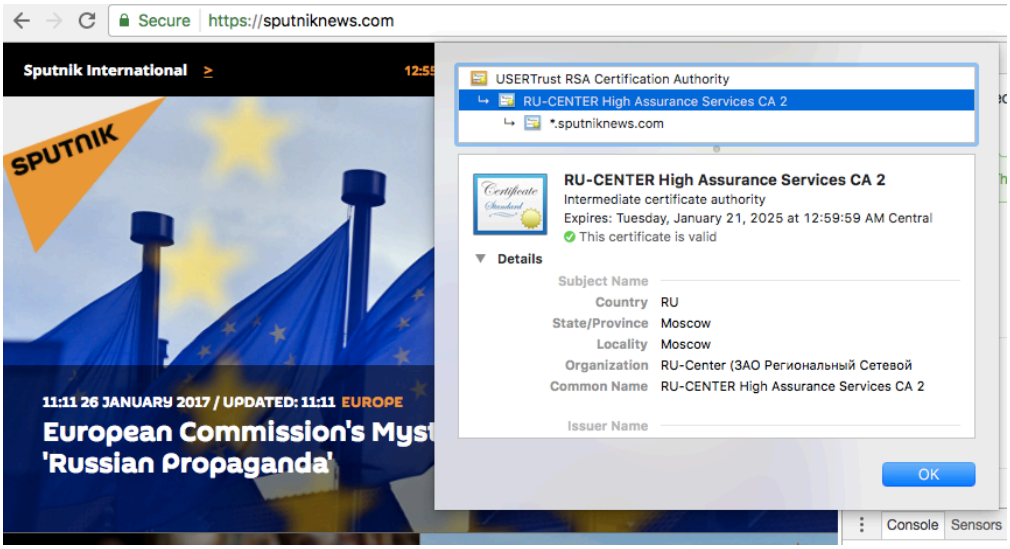
- Certificates are bought online, while local law in Serbia requires signed agreement in order to be valid.
- None of those companies are legally incorporated In Republic of Serbia, making no obligation to comply with local citizen data protection law.

This also open up a “man in the middle” attack possibility by issuer country agency, in case issuer country law permits this – even if it’s not permitted locally.



Even if Serbia does not posses trusted certification authority, This might be easy resolved using intermediate certification, that those institution could use to generate their own certificates, preventing the possibility of man in the middle as well as decryption by issuing a copy.

That's the exact case we can see, for example in Russian Sputnik:



The problem possibly affects other countries, by exposing citizen's data to foreign agencies in accordance with foreign law instead of local one.

The proposal on addressing the issue should be very simple:

Each domain that match: gov.TLD should be required to match TLD ISO code against the Issuer ISO code from within the subject section of the certificate. Otherwise, the connection should not be trusted.

The local legal incorporation should be required when putting government domains in question; as otherwise, it could lead into paradoxes such as:

- Organization level verification that might be different from local regulations.
- EV extended validation that even more misleads.

This is an issue that needs addressing at the global level, as there are no methods to force specific government entity to prioritize local incorporation (and therefore issuer liability) unless law enforces this.

However, that situation get's into collision with regulations citizen privacy protection laws that which is fully enforced.