Webinar on the future of a combined register 26-11-2018

When

26th of November 2018 11:00-12:00 CET

Where

TelCo **https://cscfi.zoom.us/j/706669343**

Please install the Zoom client in advance https://zoom.us/download#client_4meeting

Documents

- Specification prepared by Matija Puzar and Geir Vangen (UNIT, Norway) - EMREG_v2.0.docx
- Specification prepared by Wojtek Rygielski and Janina Mincer-Daszkiewicz (University of Warsaw) - migration-plan.pdf,migration-plan.md
- Specification prepared by Poland, version 2 (after the webinar) - migration-plan_v2.pdf, migration-plan_v2.md

Comments

Some initial feedback from Matija on the feedback from Janina/ Wojtek:

> *Pros:*
>
> ** Well defined, works well with existing EWP standards and protocols*
>
> ** It would solve the need for some NCPs to only accept registered clients*
>
> *Cons:*
>
> ** One of EMREX' strongest points was its simplicity, especially for clients. This way, more complexity is introduced.*
>
> ** Complex implementation*
>
> *- NCPs would need to create and handle manifests*
>
> *- clients would have to parse the EWP registry and find suitable NCPs*
>
> ** Clients would need to register in the EWP registry as well, and publish own manifests, if they are to be able to use the EWP security mechanisms (HTTP signatures are validated against known keys from the registry)*
>
> ** Missing a smooth solution to handle expiration/replacement of certificates (current EMREG is missing it too, but we have a proposal to improve this)*
>
> ** Not backwards compatible*
>
> *- rewriting EMREG to act as a proxy could work, but then it should only be that - a proxy, not have an own list in addition to the NCPs fetched from EWP; also, it would have to be a temporary solution and deprecated at a later point*
>
> ** Political issue - EMREX gets devoured by EWP.*
>
> *Suggestions for improvement, if we go for this:*
>
> ** Consider using JWT as a token (with a very short expiration time) to avoid the need to handle sessions at the NCP*

Wojtek's comments:

> *> * One of EMREX' strongest points was its simplicity, especially for clients. This way, more complexity is introduced.*
>
> *- If we go with the backward compatible solution, then not necessarily.*

- As far as I recently learned, some countries require these new features.

- The alternative proposal Janina had me read (the one about adding client certificates to EMREG) introduces even more complexities, I think.

*> * Complex implementation*

> - NCPs would need to create and handle manifests

Only if they want the clients to authenticate themselves. Otherwise, they can make use of EMREG (assuming you go with the backward-compatible solution).

> - clients would have to parse the EWP registry and find suitable NCPs

Only if the clients want to authenticate themselves. In the backward-compatible solution EMREG will do the filtering for them (and present those NCPs which can be accessed without authentication).

*> * Clients would need to register in the EWP registry as well, and publish own manifests, if they are to be able to use the EWP security mechanisms (HTTP signatures are validated against known keys from the registry)*

Same as above (only if the clients want to authenticate themselves).

*> * Missing a smooth solution to handle expiration/replacement of certificates (current EMREG is missing it too, but we have a proposal to improve this)*

It's not missing. EWP already has a solution for that. Both servers and clients are allowed to use multiple credentials at the same time. Smooth handling of credential expiration was one of the initial design priorities, and was solved long ago

*> * Not backwards compatible*

> - rewriting EMREG to act as a proxy could work, but then it should only be that - a proxy, not have an own list in addition to the NCPs fetched from EWP; also, it would have to be a temporary solution and deprecated at a later point

I don't understand. Perhaps I missed something when I was writing the quick specs draft I prepared, but I'm pretty sure it can be done in a backward-compatible way.

*> * Political issue - EMREX gets devoured by EWP.*

I guess we could dress this up in some kinder wording. E.g. "EMREX allows partners to make use of their existing EWP implementations to provide additional security, if the partners need it"

add you comments here