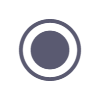
**SETTLE Discussion-20250723\_143440-Enregistrement de la réunion**

23 juillet 2025, 12:34PM

42min 27sec

 **BOUCADAIR Mohamed INNOV/NET** a commencé la transcription

 **Ines Robles** 0:03  
OK. Yes, OK. Welcome to this settle meeting. We will start.  
Can you see the slides?

 **Eric Rescorla** 0:20  
Yes, they're fine.

 **Ines Robles** 0:22  
Can you see the slides remotely? OK, so welcome. As you can see, this meeting is being recorded.

 **Eric Rescorla** 0:23  
Yes.  
Yeah.

 **Ines Robles** 0:34  
So Please note, well, the ITF policies is aligned in these meetings, so read it before participation.  
And not really well that as well. We expect the professional collaboration and networking as a defining ITA guidelines for conduct. So please read it and respect them.  
So the agenda for today, we will give an introduction, then we will speak about the chat that we have and then discuss for which are the next steps that we should take.  
Comments on the agenda.  
OK, so as introduction which is the problem definition why we once settled? Well, as you know browser requires secure context for essentialfeatures.com network struggles to get trusted certificate and that happens that the user ignore.  
Mornings. And that's not very good. And yet that become easier. So the goal of setting the goal of this working group is a great guidelines for practicals and trusted TLS deployment on local networks.  
And then OK, do you agree with the problem? It's OK for you. Do you want to discuss this?  
Oh well.  
OK, well, sorry, is this Sir Mike, I need to talk with you or I think it's only on that. I'll, I'll try to shout a bit, I guess, yeah.

 **Eric Rescorla** 2:00  
Well.  
Yeah.

 **Ines Robles** 2:11  
So I'm I'm still a little puzzled that there's a large overlap with what home net tried to do and they like after many, many years failed to get any traction on this problem. So I'm still very confused what settle things will be different.  
That they will succeed but but in home dependency second in home, there's nothing about OCD establishing stuff. I would say maybe about the establishment of the infrastructure, all the OSA Asian CP for. Often some of the naming, part delegation and so on. But there's nothing about this. So part of the home net was indeed to make it reach.

 **Eric Rescorla** 2:30  
Yeah.

 **Ines Robles** 2:47  
From the outside world, so that was part of it, but also part from the land, right? So yeah, but the communication within the land itself to why it's ensuring that we still maintain, I've said the same security level that we'll have even outside and that's nothing within the local network is not something which was covered in, you know, that's all that's for me this, this really something which is.  
Not home it at all and we are not repeating the same style that was was happening at home. It at the time. So for me it's a it's really clear in terms of this copying. So you you are not trying to build HTTPS connections to devices in your home network.  
No, those those the disablishment of the secure say communication within within your home network, this is part of the of the, I would say this proposed working book but this is not part of what was discussed I would say or explored and investigated in in home with home it is really about something which is really establishment of infrastructure how we can do.  
Litigation there you can have the naming delegation from outside inside and and and inside. All of. This is for me this is. This is how you can set up the infrastructure. The civil is a little bit in a liar above all of it. So you have your infrastructure which is really in place and now you are trying to establish a secret communication with with, with, with with say server that are within your network.  
And so and the question is, how can I trust them and how can I establish the secret communication with all these devices without accessing to? I would say devices that can be used as relief for attack from outside and all of these kind of issues. So the homnet I guess Daniel was contributing to homnet if he can.  
Or anything what I mentioned, but this is really different. OK, so my understanding to the scope of a home net was basically how you built it, but it was focused mostly on routing. And I was when I was dealing delegation with the DNS.  
It has come as a kind of artefact, but something that has not been addressed at all with security, so my understanding what home net tried to accomplish was you have established local resources in your home that you can use and now you want to use.  
From remote but you but but it had or inside, but it had all the same security problems of settle. So like settle is like a subsection of home net. But even that subsection failed in home net. So I'm very worried that like.  
That, that, that, this will, that, that, that nothing has changed and I don't think that we can get a solution. So I'm I'm very worried about what we can do. But let me just sit back and we'll see where we're where we're going. So one clarification for example is is that we never talk about certificate.  
You know on that.  
So I know for DNS SEC we try, but I mean they have what they call the HN HNCP, but we envisioned maybe some ways to distribute a key a DNS key but it has never been that far.  
For example, and certificate for TLS session or IP Tech has never been considered at all. For me, this is really infrastructure that you have doing 100 at a time. It's some kind of, I would say service discovery, but we can use off. I would say this resources and establishment here. I would say the Security Association.  
This is not something that was part of the OR investigated at, at least in the in the home. You can double check the the Charter and what you have done, Paul. But for me this is well, I mean, whether it's the Charter or whether it's part of the solution that was proposed to actually make this work, I think it will really come down to secure naming scheme, right, because that is that was the problem of home net and that is the problem of settle.  
Let's let's let's progress on the other before. Thank you very much. So about the Charter, the Charter start with the background basically stating the problem, I say well, local servers were built for encrypted connections. Modern browser requires security.

 **Eric Rescorla** 6:44  
So I have two. I have two comments about this, I'm sorry.  
I'm sorry. Can nobody hear me?

 **Ines Robles** 6:57  
Context for essential features. This make encryption and transit certificate needed even for local networks and security connection rely on TLS would use certificate fabric or private certificate authorities. Then the chart left explain yes it's in the want to.  
Yeah. Eric. He he's trying. Yeah, if you can just enable your speaker, please.

 **Eric Rescorla** 7:20  
Yeah, can, can you hear me at all?

 **Ines Robles** 7:25  
Yeah, sorry.

 **Eric Rescorla** 7:28  
Hi.

 **Ines Robles** 7:29  
Sorry, one minute please.

 **Eric Rescorla** 7:33  
Yeah.

 **Ines Robles** 7:34  
Yeah. Yes, I think they can.  
They should be able because I'm not the they should be able to. Yeah. Yeah. It's just your speaker. I can. Yes. Yes, Eric, if you can.

 **Eric Rescorla** 7:41  
OK.  
Hi am I audible now?

 **Ines Robles** 7:49  
Yes. Yeah. Can you turn the volume up a little?

 **Eric Rescorla** 7:50  
Yeah, we're just.  
Can you go back to the previous slide please?

 **Ines Robles** 7:53  
You back to previous sledding, sledding goodbye. You should turn it off. I'm gonna.

 **Eric Rescorla** 7:59  
Can you turn your turn off your microphone?  
Yeah.

 **Ines Robles** 8:14  
OK. I turn on, sorry.

 **Eric Rescorla** 8:16  
OK, go back to the previous slide please.

 **Ines Robles** 8:17  
Yes.  
One minute, please here.

 **Eric Rescorla** 8:24  
Yes. So look, I agree that like this is a real problem, but like like I actually don't think that I'm actually surprised by both the first and third points. So like most of these essential features are like advanced things. I don't understand why you need to have when you're talking to your printer and.  
As far as the Third Point, it's like practically impossible to override the browser certificate warning, so I don't think that like really people ignore warnings of the real problem. The real problem is you can't connect to these sites and like give them your password. So I guess I I I I agree. It's like a generally real problem, but I this framing makes me very odd and like like what people actually want to do with these home devices.

 **Ines Robles** 9:07  
But I think if I understand what ECHO was saying and correct me if I'm wrong, I think Echo's saying like the browsers have done a lot of work to remove all of these choices from the users so the users no longer have a choice so they don't get warnings, they just cannot connect.

 **Eric Rescorla** 9:07  
None.  
Most mostly, yeah. And as far as this first point, like what are the essential features that like you need to use here? Like when you're talking to your printer?  
Like.

 **Ines Robles** 9:29  
Like personal web transport.

 **Eric Rescorla** 9:33  
Why do you need web transfer to your printer?

 **Ines Robles** 9:35  
No, not great. Well, not well. Not not so you. You need it. It it an HTTP ads or TLS connection to connect to your devices within your ads.

 **Eric Rescorla** 9:44  
I I I I agree. But I'm just saying it's not about like browsers moving things to secure context. Somebody want to think of your password.

 **Ines Robles** 9:51  
Like I I think it I think it may be worth I think some of this is is thinking you know what are what are the things where, where, where if we had a secure secure connection that was trusted that you could get solid benefits like a concrete example would be be being able to keep to keep.

 **Eric Rescorla** 9:53  
OK.

 **Ines Robles** 10:10  
State with the device as well as have passwords associated in the password manager associated with the device in a way that they were only ever sent to that device. So like if you have like in the Web origin model, being able to have state associated with your printer like your like your password and your cookies.  
And know that once you that if if you saved that password and your password manager associated with that printer and then you're connecting again to that printer that that's that you're talking to that printer and only ever setting the password to that printer and that there's no way that a A.  
Something in the middle could then go and say, oh, I'm this thing and I'll get that. Get that stage.

 **Eric Rescorla** 10:43  
No, obviously I agree. Yes. Obviously I agree with that, but it's not what this text says. This text is all about like modern features that like we turned on only for secure context. But password management and HTTPS are like features that from the dawn of time.

 **Ines Robles** 10:58  
Yeah, I think I was more arguing for. I think there's. I think there's a bunch of stuff in the Charter that I think kind of taking a step back and looking at the Charter, not like I think there was some pieces in it that are good. But I think there are some pieces of it that spend like too much time on the context or don't really go into the here are the real concrete benefits we're trying to get or what the problems we're trying to solve.  
Yeah, we should. So, Eric, Eric, are you are you sorry, Eric, I think you're just saying that four essential features is that should be removed because it's for Oracle for functionality.

 **Eric Rescorla** 11:18  
Anyway, I'm happy to move on.  
I I guess I would. It's it's not about what's where the browsers turn on for secure contest only.

 **Ines Robles** 11:36  
Right. It's how browsers operate.

 **Eric Rescorla** 11:39  
Yeah, sure. That's great.

 **Ines Robles** 11:40  
Right, OK. We will, I think we need to the the key point is is what Eric mentioned is that some words meeting is needed there to to to be the reflect. I would say the the problem and then to avoid this kind of approximation sometimes it may be misleading for some. Yeah, I think that's for at least we have a point for this one yeah but yes. But just to clarify what's the suggestion to use the password mechanisms.  
No, no, no, no, no, it's really that. It's being able to know that if you if there's an entity you're talking to that once you've established trust with that entity that that, that you have a a identity for it that you can associate state with.  
And that future connections to that to that identity are are are authenticated so that you can know that you're talking that same identity, that same entity, yeah.  
Thank you very much.  
So basically the background they well, the chart there mentioned the background. So we we can fix that based on your comments. So make it clearly thank you very much. We will since we recorded we will take all these notes.  
And taken to the mailing list. Then the Charter as well mentioned, which is kind of this. Yeah, actually on the on the background there, I know one of the pieces that motivated that motivated this discussion was the workout of ADD to be able to specifically talk where where once you got a reference to a device.  
To a Uri for DOE being able to establish a secure a secure connection to that, I think there's a whole like how do you bootstrap that, which is probably out of or at least is a separate question, but that aspect of being able to get a Uri for something like a DOE server.  
Via if you got it via DHCP, being able to then securely authenticate to that is certainly a A use case. It's there was one of the driving motivation.  
Yeah, and yeah, this is the I think this. Yeah, if are there services area that we need to mention and also in this in this in this part or we don't have to be exhausted actually. But yeah, I'm just trying to think of like things where where we should be, it might be worth trying to think of what are the properties we're trying to get out of this as and and what properties can.  
We get out or what? Can't we get out? Because I think that there are. I think this goes to the point Paul was making earlier of solving. There's an overall magical scope that's not tractable to solve. But if we're willing to make a set of compromises and say things like, OK, once you've done tofu, trust.  
Making it such that any state associated with the thing you're connecting to is. You're gonna have a aestheticated and secure connection there. There's a class of these problems that are that are do have a kind of a reasonable trust, a reasonable scope bound that seemed tractable. So trying to figure out which are those.  
And make sure that the kind of the background of those use cases cover the ones that we think are clear to solve, and we may even want to think about which in the Charter think about which are the parts. The problem that we don't think are that we think are possibly too big to solve and therefore what it could have put out of scope like like for like it just as an example.  
Being able to have that part of some global namespace such that someone you could connect to your printer from outside of your home and be able to print to it is clearly the out of scope category yeah, from which it seems really reasonable. And for the other part you mentioned about, it's an accident from outside and so on.  
Just joined the discussion we had about home because they have all these issues, but yes, you are completely right that we have really to to restrict the scope is that's something that can be really tractable. OK, thank you.  
And continue well, the Charter as well mentioned which is the status, the product that we have when we have public certificate authorities for example local service can easily get the certificates because they are sometimes behind firewalls. Now they don't have powering DNS names.  
And these certificates needs renewal. So we are the trusted certificate. You still get warnings every time they connect and over the time while you still get in order requirements which make a prone to attacks.  
And then the draught continue with the when it's locally installed certificate authority. What happened and it's not very, very hard for users to use it on manners they don't know sometimes how to create an installed certificate request. Many device can create this request and as well as certificate need to renew one and.  
Browser and OS handles private certificate authorities differently and then as well it's a lot of risk that they can be misused to insert web security connections on any networks then they charted.

 **Eric Rescorla** 16:27  
So so can I can I would just cut a lot of this motivation. Frankly, I have disagreements that a number of the statements made here, but I agree this is a real problem. So like both in this slide and all three of these slides just need a lot less because like.  
Well, it's just like because otherwise you'd end up arguing about the truth value of a lot of these statements. So a lot less would be helpful.

 **Ines Robles** 16:51  
Yeah, I like. I think this is my biggest concern. That was one of my biggest challenges with the Charter is because over half the text of the Charter is on. Here are the things that don't work. I think that if as a quick like the quick read through, it's very easy to get distracted by that and to think that's what it's about and and.  
And since some of these problems are are well known enough, having it just be a kind of condensing both those two sections down into even 2 bullet points of the alternatives that the alternatives to settle that don't work that don't work well in these contexts are public certificate authorities and locally issued CAS.  
And if we need to, we could either have a reference off to other things that have that, or or have at most one sentence for each one explaining why it's a problem but not have a whole section on it. Have these words. Yeah. Yeah. OK. So we want to exclude.  
A local CA, for example. No, no. In the in the chart. I think that's what error was. Imagine that we don't need to to to go into specific. I would say solution or even some issues because otherwise we'd be distracted and having less word on the context will be helpful. I would say to frame I hit the probably if that's exactly what you have mentioned. Yeah. Eric. Yeah. So but but to a point.  
Sorry but but to a point there is that if you're going to design a new security protocol, we would have to be really sure to that. This goes into the SEC area because otherwise you you will not get feedback from the security people who will have conflicting meetings with your meeting. If it's an OPS. Yeah. But there's no specification of protocol here at all.  
In the first stage of the working group, there is no work specific. No protocol work. Yeah, it's next slide. There is no protocol work, so it's only using existing problems. Yeah, this is how the goals basically primary goal is to provide implementation and operations.  
Guidance to obtain secure context with service operating in the local network. So all the protocol change or extensions are not part of this working group. They are going to be part of another working group. But of course we're going to be reviewing and have a new discussion with the specific working groups.  
To fulfil the first goal, then as well the working group may consider assessing the applicability of the guidance for a few services. We will concentrate on unique host names.  
Yeah. And actually just one comment about the assessment of the new services. This is when it comes some of the services you have mentioned, that's why it is important also to identify some of them that we would think that are really important to show that this will work for this guidance and there will be a discussion on which are those services that we think are work to be to be considered by by the proposed.  
Working.  
I guess there's a question. I guess there's a question in this and this kind of goes to that other one of of.  
If there's a the the the shapes of this problem that might. I think the old like. There's like there's certain shapes of this problem that are solvable, and there's certain that aren't solvable if there are directions that we think that are needed to make this tractable, like an example would be the.

 **Eric Rescorla** 20:25  
Yeah.  
Yeah.

 **Ines Robles** 20:25  
And then having the working group go off of that rather than rather than having it be so open-ended that it gets back into these discussions of, oh, how could we get public CAS to issue things for dot local 9 names or private IP addresses, which is kind of a deep kind of like this thing that's been retreaded over so many times and isn't tractable.  
OK, so the next important thing that we have to discuss, whether we can include at least some simple examples to show that this is solvable and we need to find to figure out those to be merged in the chart or not. So we can have this, I would say as a further discussion we'd have on the mailing list.

 **Eric Rescorla** 20:57  
What?  
But but I don't understand, none of this is guidance. What Eric is posing is new is new technology, right? And so this is my problem with this entire text is this problem is not solvable this in technology. So new technology has to be invented and so none of this makes any sense because the only thing that makes any sense is .2 and.

 **Ines Robles** 21:01  
Do we have whiskey?

 **Eric Rescorla** 21:19  
And .2 gets right back in the problem I was saying before, which is you can't design this in a vacuum without cooperation for the people who actually have to do the work. And those people seem interested. So I just understand what the point of this any of this text is supposed to be.

 **Ines Robles** 21:32  
Right, So what I'm also thinking of the use cases like like so like the three simple, not simple. The three common use cases that I'm thinking of is one you need to reconfigure your home router, so you need to web browsers to your home router to reconfigure it. And how do you do that properly? Two is like you know, how do you?  
How do you print something and three is like like, you know, I need to transfer a file to my wife's laptop and I want to basically AirDrop it in a standard way that doesn't require specific operating system extensions, but those are completely different technologies, completely different things, only like one of them is like like finding my, my, my wife's.  
A laptop will be something of local broadcast announcements. Finding a name hoping that nobody has the same name with the other laptop, or things like that. So that's a completely different thing from connecting to my router, which there might be different standard spaces there where we go. Maybe we can offer some sort of standard solution.  
Where you know like this is the advertised networks router configuration page like. I don't know, it could be the HTTP option for all I care right? Like this completely different space. So I'm a little confused how all of this sort of boils down to one settle working group thing.  
So you mentioned connection to the router.  
So you mentioned connection to the router, a file transfer. What is the difference between a file transfer and an HTTP connection for you? Ask for example. Or is that the same? It's completely different based on the. How do you find the device you're looking for? Yeah, yeah, yeah. If you want to transfer.  
The problem between my phone or my laptop or my file server, you get them to the school like technology. You first you need to decide the technology, but first you need to find these devices and that it in itself is different technologies. There's a bunch of that that does have an ecosystem of things that's and like MDNS is an ecosystem for and we have.  
And I think there's some common grounds here that we want to scope in like this is for like TLS or maybe even maybe even say this is about HTTPS or some. And then if I think narrowing down the scope of protocols from the broad it could be anything to at least.  
TLS based product TLS based protocols including HTTPS. We can just start with HTTPS and that, but I think that to solve this I think it there is going to be a some security. There's a lot of the problem is going to be that security engineering part of this. So there may be a.  
I think there may be a good question of should it just start off in SEC area to focus on kind of because it's not really just an operational issue. If it was an operational issue, I just glue a few things together. It would be a different story. But here I think it's going to be figuring out kind of security model wise how do we.  
How do we get kind of whatever those names cryptographic identities are that show up in that might kind of be advertised in MDNS, and that you might trust on for excuse. How do you get those such bound in such a way that?  
That TLS that TLS stacks can can can do that server authentication in a way that does not compromise the rest of the ecosystem, and that could be introduced into browsers and other clients in a way that was minimally disruptive.  
So the principal, so the principal should be looked at in this working group and then the design of specific extensions to maybe I mean TLS or whatever working group it is so but but the strange thing I think about that is this that it is it is like it's not.

 **Eric Rescorla** 25:12  
But that's not gonna work.

 **Ines Robles** 25:18  
They've known that the other groups have not worked on it. They probably either haven't worked on it for a good reason or they're not interested, or it's too complicated that they haven't solved it. Like everybody knows these problems. And if this working group's only output is to say, these are the problems, how do you guys go fix it then? I'm not sure if that's a working group.  
Yeah, 'cause, it's the the hard the hard problem is going to be a lot of it's going to be that protocol design and how that protocol design fits into the ecosystem from a security perspective like that's the kind of the meat of the problem. And just putting together and the any requirements document or other operational documents that aren't put together.  
Kind of in parallel with a design with iterations on like. Here's what is and isn't possible and iterating on until you have kind of a set of requirements and a proposed solution that actually solves those requirements isn't going to it's just going to, isn't is not going to be worth time.  
So what we are suggesting that in addition to the current scope which is limited, I would say to the to the excluding the solution space is that you are suggesting that also the solutions can be part of this and then if this is part of this then naturally this is not OPS anymore. This is elsewhere. But this is so you're sorry, we need also to discuss this.  
That, that, that option as well. Yeah, I think in order I I think in order to be tractable, it's gonna need to have a that coming up with a solution space in liaisoning with with TLS probably with W3C possibly with some others on that technical on that technical solution based on the on the requirements.  
OK.  
You can just move move on to the next slide and when you have the movements of the items from OK, the problem of work well. Develop a document describing the problem and the templates of the problem and the problem issues as well.  
We want to develop a requirement documents that balance existing browsers behaviour and then operational guidance for deployment of a system. That means the working group first goal and the develop applicability for operational guidance.  
2K applications that may be selected by the working group, so it's what is expected then yes, the Charter as well mentioned the coordination as Eric was saying with RSD OS like W3CG SMACA browser forum.  
Among others in the many history were mentioned IOTSF and others we will consider as well that.

 **Eric Rescorla** 27:49  
So so I want to step back from this text. What is your theory of change here? Like the underlying problem as Eric and I have both told you, is that you need to change the browsers and that means you've needed something in TLS or or some other working group like that. Right and.  
As Paul said, none of those people have worked on this problem or they have worked on it, concluded it can't be done. So what is your theory of change for what is going to happen that is going to actually get this done because you can run as many documents as you want, but until someone actually solves this problem with an answer that's acceptable to the browser vendors.  
This is dead in the water. So what is your theory of change?  
Don't tell me about your charter charter ball stones. Tell me your theory of change.

 **Ines Robles** 28:25  
Yeah, yeah, yeah. The the main approach here is that if we attack directly, I would say this the the solution space without having disagreement on what we need to to be solved and what are the the key requirement that we are seeking for it will be difficult. I would say to have that solution in place so that preparative work to understand exactly.  
But what is the problem we're trying to solve and the set of key feature that that are missing. This is really primordial and it's not shall for for this work that's so this is really phasing, but you're not solving.

 **Eric Rescorla** 28:52  
OK, so so your so your theory is your theory is that the hundreds of pages that have been written about this have not flushed out enough. That's your theory.

 **Ines Robles** 28:59  
Yeah, but there is, yeah. The the key point here is that there is no sort of consensus of this kind of aspect. Everyone can have his his own opinion. You can have your own. Eric. Eric. The other, Eric, have this opinion. Me too. I have my own opinions and the others. But you're not. So you're not solving or trying to.

 **Eric Rescorla** 29:11  
Move the problem.  
OK, but the problem is the over constraint.

 **Ines Robles** 29:16  
You're not trying to solve one problem. You've identified various problems in various different areas, and the only common factor is that there is an end user that cannot do this. But that's not a binding factor for work on a working group. It is if we tell, for example, what Eric said, you said about better scoping into something kind of tractable. This is for me.  
There is an approach that you can do together and I understand from for example, that he has already identified some item in the Charter that can make this be bitter and bitter scope. So I think that we can work on something there to better, I would say identify that space and not just boil the ocean or I will try to solve everything but keeping really something.  
Really have your focused and I think there is there is a path for that for that at least what this is what I'm hearing for some of of young also in the past on the main list. But I I I think I think.

 **Eric Rescorla** 30:03  
Well, you haven't heard from anybody. OK, but again, like a lot of work has been put into this by a lot of people who understand the web PPI and the browsers very, very well, right. And they've all, like, run up in the same kind of problems and all kind of run up against the same kind of solution. Eric is Eric is proposing here. Right. And then it just kind of stalls because nobody finds it very interesting.  
And so like like like if you and and the problem is they don't understand, not that they don't understand it. The problem is over constrained. And so like if you want to get through that you need to scope down. You need to do 2 things and you scope down the problem enough that it's actually tractable. And then you need to build consensus among the people who actually can make the change.

 **Ines Robles** 30:26  
But.

 **Eric Rescorla** 30:42  
Which is to say, the browser vendors that they will adopt it and so I don't see any of that. What I see is you issuing a work order to the browser vendors, which they're going to ignore.

 **Ines Robles** 30:43  
Hmm.  
Yep, just to let you know, some of the discussion, I would say we had offline some of the browser vendors, some of them at least they are interested what they told them that they are interested in what comes after Seattle. That means that in the solutions extensions, but they are not bringing this to the list because we are focusing here currently on the, I would say this kind of defined requirement.

 **Eric Rescorla** 31:05  
Yeah.

 **Ines Robles** 31:11  
And so on. So it it's it's just a matter of. So it's a decision for us as a group. We do. We think that's it's.

 **Eric Rescorla** 31:15  
Well, I I I guess I'm not. I'm not really moved by some people I've talked to offline or in favour of this, like, let them show up but like but again the problem is you need to scope down the problem and that needs the input of the people are going to implement it. You can't just be like rescoped it down in a vacuum. Go do it. You need them to come and say we could do this and we can't do this and that tells you what problem parts of the problem.

 **Ines Robles** 31:23  
Yeah. Yeah, that's.

 **Eric Rescorla** 31:35  
You can solve.

 **Ines Robles** 31:37  
Yeah, like I think in order, I think in order for this to be successful, this is going to, for example, need someone from Chrome who's has time with a dedicated time to work on this to to be engaged. I think the half the problem with this has been running to is lots of people agree that there are there's an important problem.  
There's a lot of people who have kind of had ideas like Martin Thompson's written up stuff over the years, but but it's never it's never become something that it's hard to get people, including myself, to actually be able to spend any time on it because it's it's it's hard to figure out how is this part of People's day job, what business problem is it solving for the.  
Who would need to have this be enough of part of their day job to spend to get spend enough committed time down it to get over the wall? So I think it'll be really important for it to be successful is to get like someone from Chrome to get in to say yes, I'm gonna get involved in this. I'm going to go to kind of.  
Focus on working with the working group to find a solution that's viable. Just putting a bunch of requirements over to Chrome will just be A and other browser is probably going to be a waste and set of effort. I think it's it's very common when we have a problem.  
It is when we say, yeah, we're going to make some requirements. Requirements must be, I mean make sense. So. So that's also part of this group to find out if there is a solution that can make sense and what without the.  
Extension impacts, but I agree that we will have to to engage with the the, the the web browsers, but I would say once we have a clear idea on how we can scope the problem and how we can, what we know, what we are going to ask for that's that's what needs to be done.  
Settle if we say yeah, we can solve that without any change. Perfect. Because TLS is one thing. A lot is one other.

 **Eric Rescorla** 33:35  
But you know you can't, right? You know you can't come up with any change like that's already known. So again, the point I'm trying to make is you can't that in order to scope down the the requirements analysis in a problem like this, like you have a big set of requirements and you remove some. And the only way to remove some is to know what's practical, what's not practical, and that requires.

 **Ines Robles** 33:41  
Yeah.

 **Eric Rescorla** 33:54  
Players having the constraints discussion with the people who are actually going to build the thing so you can like. Otherwise you're just guessing what, what, what they what their constraints are. So you actually need to have them involved.  
And if you, if you're telling me they won't be involved until you have until you have this done, then like you're done, like you're not going to succeed.

 **Ines Robles** 34:05  
Like I didn't.  
Yeah. And I think I think a big part like a huge part of this is going to be the user experience like it like that that I think is going to be a massive challenge in getting forwards here. So it may. And I heard second hand from someone that this was being discussed in W3, CT pack recently.  
So this might be something of of of figuring out working with W3C to figure out how do we have AW3C side of this and the ITF side of it and factor like Mark has been doing that successfully of having W3C here. Here is 0 scope on the of the user experience in the browser APIs.  
And ITF is at a protocol level. It may make sense for for settle do something similar of how they be paired up with the W3C working group that's working on the user experience side of it. And then IBF is working on the on the protocol on the protocol side of it.  
But I think just starting off with requirements without having some pairing like that May may maybe isn't going to get a lot of those important user experience requirements.  
OK. Thank you. We continue.  
So these are the proposed milestones for September of this year. Simulations to identify organisations SDO that we agree in the working group. Then in December submit the promised statements.  
And the payment issues to the ISD for February next year will be to submit the requirements to the ISD. Then for April next year to submit the operational guidance to the ISD and then in August.  
Close or a charter?  
Comments.  
I'm not. I'm not sure what operational guidance would be here because there's no like until you've actually designed and built something and have and actually have developed a protocol. There's nothing to give operational guidance on an example. For example, if you have a, if you have a dentist forwarder, for example, if you have a home.

 **Eric Rescorla** 36:00  
I mean, these are just milestones, so things you shouldn't do so.

 **Ines Robles** 36:16  
Want to establish, for example, a secure context with that one, there will be something that need to be done. I don't know so far if it is specific or not, but at least it's a go there to show practically how you can do it in order to establish I would say the end to end. I would say communication that would be all.  
Thinking the forwarder, why you maintaining the encrypted dens in all legs? That's just one example, but I I don't know what what other aspect that we may include, but just to give you example, what what is behind this kind of sentences.

 **Eric Rescorla** 36:44  
I I'm sorry, these are these are just fantasy, right? So, like, if if this could, if if you could publish operational guidance next April, then the problem would already have been solved and it's not solved. And so like I don't understand how you think that you're going to go from nothing to operational guidance as Eric's as a protocol doesn't exist in what in, in, in, in.  
Ten months. That's just, like, not plausible, right? Like for a problem that's been being worked for five to 10 years already. Like, I just don't understand, like, how this possibly could happen.

 **Ines Robles** 37:14  
OK. That's that's that's a pair point because this depend actually on the requirement other to the analysis of the you said that's a this perform.

 **Eric Rescorla** 37:20  
I mean, I mean, I mean the the the absolute best case scenario here is that you come down with some reduced problem statement that you then take to the people after do the work in the in the in the security community and they take a year or two to to to work with the problem and another year or two to implement it. And you're like two years down and then you have a thing that actually.  
Worked and then maybe some operational guidance, but that's like that this number should say 2028, I mean not 2026.

 **Ines Robles** 37:49  
OK. Thank you. We will anyway they.

 **Eric Rescorla** 37:50  
I mean, I mean, I don't, I don't think that. I mean I don't think these are good milestones anyway, but the numbers are just like really kind of like science fiction.

 **Ines Robles** 37:58  
Yeah, I'm taking consideration that the milestone going to be updated as we see how the working group is move and advance. So it's.

 **Eric Rescorla** 38:05  
Well, I I I know, but just like, but just like, right down, right down the right down like the actual timeline and you'll just see this can't happen.

 **Ines Robles** 38:12  
But yeah, I think also the the items on the timeline like really depends on where the Charter goes because the Charter will completely change all of these timeline entries anyway. So I think also this is sort of fantasy.

 **Eric Rescorla** 38:22  
Right, right. I mean, I mean, I mean the working was not even gonna be the working was not gonna be formed in the best case scenario until like December 2025.

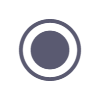
 **Ines Robles** 38:29  
OK. Thank you. OK, thank you. We will take that in consideration. We move to the next slide. So basically, just as a overview of the Tata Tata tracker, the Middle East was created last year and they are for related Internet draught.  
So a referee don't indicate servers in local domains. Public key hash for local domains. Requirements for HTTP for local domains, and Acme for IoT device. So this to me again feels like there's a solution. Somebody has a solution in the back of their mind that's not clear at all to me about the Charter and the problems like.  
In fact, that there's like some sort of protocol with a referee and an authentication handover. This seems like very much a solution that I don't see can work at all or might not be needed. If it's like a peer-to-peer in a network like my laptop to my phone doesn't need a third party referee, or if it does like you already have Bluetooth devices doing this kind of thing. So we shouldn't like invent our own thing with a third.  
Party. And so I think there's already specifying solutions that I think a lot of people not agree with.  
This are individual contribution, so right. Yeah. Yeah. There's people they said, yeah, they got under the root. We've never been off. Yeah.  
OK. Thank you. And then next steps, so do we do we have, do we want to have regular interim meetings? I think that is the idea. Do you agree with that? I think I think one of the key points here is where to start from what Eric mentioned.  
It's really start scoping the problem to be something which is really tractable and simplify the Charter to have to to be less, less worthy to and and avoid the distraction there. Once we have, I would say that part which is which is worked out, then we have, we'll have the discussion whether the solution space should be also inside within this working group or not.  
So that's something that we need to discuss based on that outcome of discussion, then we can have more logistical aspect. But I think we have at least two items to do simplify and work out the Charter then have the discussion about whether we can include the solutions aspect or not of it. Yeah. And I think from that it'll also fall out which of those draughts are actually in scope for.  
Which of them are should you have to spatch someplace else? Yeah, yeah. And also a point about the nuisance. But that one, we cannot do it without having a formal working. So we are just, I would say, the chicken and the egg stuff. So, but this is.  
Important we'll try to see if these people, for example, The Who attended the TPAC meeting and so on, if they can and we say show up in the in this in this in this working group and see if we can have obviously voices on this. But that's going to be it depends on the how things would be a model for the working.  
Yeah. OK. So intermittent. Do you worry without to add? I think it should be good that we can continue having this to to to to further to the, I would say the Charter and then and yeah just I would say based based on that for the next steps so August it's OK for you.  
Well, we can't lay in the Middle East, OK?

 **Eric Rescorla** 41:26  
I I I I sort of like you can you can work with this Charter as much as you want but like you have actual fundamental substantive problems here with what you're frozen to do and no charter testers going to fix those. And so the most important thing as I said at the very beginning is to actually get real engagement from the people who can actually do the work on this.  
And without that, like like one of the main questions we always ask is can we actually achieve this and is there a community of interest and the fact that you want this is not going to get that done. What we'll get that done is the people actually do the work being involved. And so it's like like that's the most important thing and all this other procedural machinery, if the Charter is just like not relevant until you get that problem solved.

 **Ines Robles** 41:49  
No.  
OK. Thank you.  
Some additional comments or questions.

 **Eric Rescorla** 42:06  
Yeah.

 **Ines Robles** 42:09  
OK. Thank you very much for your attendance. We will let you know later where is the link with the recording so you can access to them and we will update the notes and let you know. Thank you very much. Thank you.

 **BOUCADAIR Mohamed INNOV/NET** arrêt de la transcription