ROW13 Transcript
June 4th, 2024, 13:00 – 17:00 UTC

Registration Operations Workshop

regiops.net

1
00:00:02.340 --> 00:00:13.759
Steve Conte - ICANN Org: This recording will be available on the ready Ops website at some point after this session, it'll take a couple of hours to get there. So with that, please welcome again?

2
00:00:14.630 --> 00:00:27.199
Hadia Elminiawi: Thank you. And welcome to the 13th registration Operations workshop. My name is Hadya Elmania, and I am delighted to be with you today as the moderator of this workshop

3
00:00:27.590 --> 00:00:41.280
Hadia Elminiawi: as we celebrate Rose 10th anniversary, we would like to begin with a heartfelt thank you to the entire community that has successfully driven this journey for a decade. Now.

4
00:00:41.380 --> 00:00:49.230
Hadia Elminiawi: your dedication and collaboration have been the cornerstone of our progress and achievements.

5
00:00:49.390 --> 00:00:53.449
Hadia Elminiawi: Today we continue a role journey together.

6
00:00:53.560 --> 00:00:58.969
Hadia Elminiawi: focusing on the critical technical aspects of registration operation

7
00:00:59.080 --> 00:01:04.960
Hadia Elminiawi: operations. Let's make this workshop productive, insightful and memorable.

8
00:01:06.400 --> 00:01:09.410
Hadia Elminiawi: if we can get this next slide, please.

9
00:01:13.560 --> 00:01:18.720
Hadia Elminiawi: So here's a list of our panelists for today.

10
00:01:19.379 --> 00:01:33.610
Hadia Elminiawi: Unfortunately, Pavel from Dnick is not feeling well and will not be able to join us but however, Michael Polage is kindly filling in for him.

11
00:01:34.220 --> 00:01:44.979
Hadia Elminiawi: please note that the detailed agenda and presentations are linked to the row, 13 agenda available on the Row website

12
00:01:45.750 --> 00:01:48.010
Hadia Elminiawi: if we can get the next slide.

13
00:01:52.710 --> 00:02:11.780
Hadia Elminiawi: So Kofomo, the consulting and development service services firm and the organizer of row extends its heartfelt thanks to the sponsors of Row 13 and the Row series very sign, and I can for making this event possible.

14
00:02:12.206 --> 00:02:33.980
Hadia Elminiawi: Please note, as as mentioned before, that this session is being recorded, and that the recording will be available on the road website within the next 24 to 48 h we also kindly ask ask you to adhere to the expected standards of behavior during this session.

15
00:02:34.397 --> 00:02:41.079
Hadia Elminiawi: You can find you can find them in the chat window and on our website

16
00:02:43.090 --> 00:02:46.079

Hadia Elminiawi: if we can move to the next slide, please.

17
00:02:46.750 --> 00:02:48.420
Hadia Elminiawi: That's the agenda.

18
00:02:54.250 --> 00:03:13.020
Hadia Elminiawi: So again, the presentations are available on the road website on the agenda and the agenda includes 6 individual presentations, a panel on the implementation of Nis 2 directive.

19
00:03:13.473 --> 00:03:29.999
Hadia Elminiawi: We have a 15 min break in about a couple of hours a a 20 min open discussion, and we have allocated 20 min for open discussion at the end of the session. If if time permits, of course

20
00:03:30.676 --> 00:03:52.583
Hadia Elminiawi: please also note that all attendees will are being muted to allow speakers to communicate without any background noise as mentioned also before, we welcome your questions and comments at the end of each presentation. For this, you can use the QA. Pod,

21
00:03:54.010 --> 00:04:19.590
Hadia Elminiawi: and however, in all cases to create an an interactive session. And if time permits, I will unmute your mic, so that you may ask the question directly to the Speaker. Questions that cannot be addressed on the microphone due to time. Constraints will be answered directly in the Q&A window, or by email.

22
00:04:20.975 --> 00:04:40.370
Hadia Elminiawi: Of course. The presentations are are 25 a minute long, and we'll include a QA. So also you're welcome to raise your hand at the end of the presentation or at the end of the panel discussion.

23
00:04:43.330 --> 00:04:49.189
Hadia Elminiawi: We can move now to the next slide, so we will begin

24
00:04:49.640 --> 00:05:14.580
Hadia Elminiawi: the workshop with Sophia Silva bar Barangu, Rpki program manager at the number resource organization and Brad Gorman, a senior product owner routing security at the American Registry for Internet numbers. Aaron, the title of their presentation is collaborating to advance. Rpk.

25
00:05:14.580 --> 00:05:18.977
Hadia Elminiawi: I. New initiatives and global progress.

26
00:05:20.420 --> 00:05:32.829
Hadia Elminiawi: Sophia and Brad, you have 20 5 min allocated. This includes the Q&A and Sophia. The floor is now yours. Please start. Thank you.

27
00:05:33.860 --> 00:05:45.370
Sofia Silva Berenguer: Thanks so much, Hedia. Hello, everyone. My name is Sophia, and I'm the new annual Rpk program manager, as Hidia mentioned. This is a joint presentation with Brad Coleman from Aaron.

28
00:05:46.357 --> 00:05:48.030
Sofia Silva Berenguer: Next slide, please.

29
00:05:48.130 --> 00:06:05.840
Sofia Silva Berenguer: The title for my part of the presentation is a more consistent rpk, I service for the global Internet community. Which is a very brief summary of what we are trying to achieve with this new program that I will be talking about today for the next 10 min or so. Next slide, please.

30
00:06:09.190 --> 00:06:18.210
Sofia Silva Berenguer: And I thought, before I talk about the program, the Rpc. Program in particular, I would briefly introduce the Nro, because not everyone may be familiar with it.

31
00:06:18.651 --> 00:06:34.709

Sofia Silva Berenguer: The Nro is the number resource organization. Some of you may be familiar with Aarin, which is the regional Internet registry for North America and some parts of the Caribbean as well as Arin. There's other 4

32
00:06:34.710 --> 00:06:54.170
Sofia Silva Berenguer: regional Internet registries for the other regions of the world. And these 5 R. Are brought together under under this organization with the mission of actively contributing to an open stable and secure Internet through different initiatives in the space of Internet governance, but also in the space of technical coordination.

33
00:06:54.670 --> 00:06:56.049
Sofia Silva Berenguer: Next slide, please

34
00:06:59.570 --> 00:07:02.689
Sofia Silva Berenguer: and before going into the

35
00:07:02.730 --> 00:07:15.260
Sofia Silva Berenguer: background or context on how the program came about. I did want to touch on why, we think this program is important. So some challenges that we are aware of, although there's probably

36
00:07:15.340 --> 00:07:16.610
Sofia Silva Berenguer: different

37
00:07:16.650 --> 00:07:17.240
Sofia Silva Berenguer: Erm

38
00:07:18.290 --> 00:07:40.869
Sofia Silva Berenguer: areas or different opportunities that could benefit from better collaboration and and coordination among the 5. Irs, there's some challenges, challenges in particular that we are aware of, and in in particular we are exploring the like diversity or inconsistency that may exist nowadays. So although in the title of my presentation I talk about

39
00:07:40.870 --> 00:08:03.820
Sofia Silva Berenguer: Rpki service in singular in practice, each Ra has their own implementation of the Rpki system, and we are aware that there's some differences, and in some cases diversity may be a good thing, maybe even welcome. But there may be some inconsistencies that may present a challenge for for some participants of the Internet ecosystem.

40
00:08:03.820 --> 00:08:10.699
Sofia Silva Berenguer: So some examples that I have included in this slide some examples that have been documented is

41
00:08:10.990 --> 00:08:12.450
Sofia Silva Berenguer: around different

42
00:08:12.928 --> 00:08:39.700
Sofia Silva Berenguer: services or features that may be offered in different ways, or maybe offered by some irs, but not by by others, or some characteristics of the system, some design decisions. That maybe slightly different from r to ir. So some of these differences are documented in a manners document that compiles some like requirements and and standards

43
00:08:39.700 --> 00:08:59.940
Sofia Silva Berenguer: for the operators of Rpi services. So, for example, the Irs, and in an annex which is a bit old, and we will be working on on an updated version of this table. But just as an example, the Annex shows how the different Rs may be compliant or not with those requirements and standards.

44
00:09:00.470 --> 00:09:01.900
Sofia Silva Berenguer: Next slide, please.

45
00:09:04.460 --> 00:09:09.410
Sofia Silva Berenguer: So, as I mentioned, we are currently focused on exploring inconsistency.

46

00:09:10.382 --> 00:09:12.370
Sofia Silva Berenguer: Next slide. And

47
00:09:13.340 --> 00:09:24.479
Sofia Silva Berenguer: what we are wondering is whether that inconsistency among the rais may be representing, maybe hindering, the adoption of Rpki.

48
00:09:25.790 --> 00:09:28.899
Steve Conte - ICANN Org: Bear with me one second, please, Sophia. Nicole dropped.

49
00:09:29.696 --> 00:09:30.309
Sofia Silva Berenguer: Don't worry.

50
00:09:43.810 --> 00:09:46.930
Steve Conte - ICANN Org: You are. Do you remember what page you're on? I'm gonna go slow.

51
00:09:46.930 --> 00:09:50.610
Sofia Silva Berenguer: Not by number. But yeah, if you keep going, I'll let you know when to stop.

52
00:09:51.400 --> 00:10:12.309
Sofia Silva Berenguer: I was just using that slide. So what I was saying is, we're focused on exploring those inconsistencies or differences across the Riis. But the main, like philosophical question, is whether those differences are currently hindering the adoption of Rpg. And whether there's something that we could do to improve that situation.

53
00:10:12.490 --> 00:10:13.970
Sofia Silva Berenguer: So next slide, please.

54
00:10:15.230 --> 00:10:34.710
Sofia Silva Berenguer: So now, stepping back a little bit I did want to share how this program came about. So in 2,022, the Nro went through a strategic

review process and apart from other outcomes, there was an agreement to work toward providing a robust, coordinated, and secure Rpki service.

55
00:10:34.790 --> 00:10:49.909
Sofia Silva Berenguer: So as a consequence, this Api program was created, and we agreed that the the purpose we wanted to start working towards was to provide a more consistent and uniformly secure, resilient, and reliable Rpgi service.

56
00:10:50.030 --> 00:10:55.639
Sofia Silva Berenguer: So in particular, we hope we will be removing some barriers for adoption, that

57
00:10:55.840 --> 00:11:04.429
Sofia Silva Berenguer: network operators that are interacting, creating certificates and grow us through the different through more than one Ir could be experiencing.

58
00:11:04.810 --> 00:11:06.319
Sofia Silva Berenguer: Next slide, please.

59
00:11:07.220 --> 00:11:18.460
Sofia Silva Berenguer: The program team for this Rpki program consists of 1st of all, the Nro Executive Council, which is the executive sponsor of the program. And

60
00:11:18.460 --> 00:11:40.979
Sofia Silva Berenguer: it's basically the 5 Ceos of the 5 R. Irs. As I mentioned, I'm the program manager for the program, and I'm working closely with Rpi experts from the 5 RS. Which we call that that group the Rpg steering Group. And we will also be working with the with different Rpki subject matter experts.

61
00:11:41.341 --> 00:11:47.130
Sofia Silva Berenguer: Outside of that steering group, and some other Api Smes from the R. Ir. As well.

62
00:11:47.820 --> 00:11:54.750
Sofia Silva Berenguer: Brad Gorman, who will be presenting after me as part of his joint presentation, is part of this Api steering

63
00:11:55.160 --> 00:11:56.500
Sofia Silva Berenguer: next slide, please

64
00:11:58.153 --> 00:12:11.480
Sofia Silva Berenguer: and as I mentioned. The purpose of the program is to provide a more consistent and uniformly secure receiving and reliable Rpi service. But that's a very broad purpose. So the 1st few months of this year when we were

65
00:12:11.660 --> 00:12:34.010
Sofia Silva Berenguer: launching or kicking off this this program, I focused on having conversations with the steering group, trying to agree on. What are those more specific, more specific outcomes that we could start aiming for? And so the 1st one, and probably most important, is, we want to really understand what a single global Rpi system looks like

66
00:12:34.010 --> 00:12:47.679
Sofia Silva Berenguer: from the perspective of the community, want to understand what are the expectations of the technical community in terms of consistency in terms of thinking of this whole Rpg system as a single thing.

67
00:12:48.059 --> 00:13:10.240
Sofia Silva Berenguer: And then there's some specific aspects of the system that we will be trying to understand and and better document one is robustness. So we believe that the community would like to have a better understanding and more transparency around different aspects of robustness of the Rpki system. So we would be working on that.

68
00:13:10.240 --> 00:13:25.820

Sofia Silva Berenguer: And, of course, security is a focus nowadays, I think, for most of us is, but we do want to do some work on enhancing the consistency of the security of the Rpg. System across the different rs.

69
00:13:26.140 --> 00:13:41.380
Sofia Silva Berenguer: and then, finally, where most of my work is, is our last arguments around keeping the community informed and engaged throughout the program. And also being able to address any concerns raised in a more coordinated way.

70
00:13:41.720 --> 00:13:43.210
Sofia Silva Berenguer: Next slide, please.

71
00:13:44.610 --> 00:14:09.419
Sofia Silva Berenguer: So I talked to our consistency. And and one thing we want to acknowledge is that we are that there are different aspects of consistency, right? So we could talk about consistency at the level of services and features offered, or we could all talk about how they are offered. So what's the mechanism in? In, for example, in the case of an Api, what's a different api endpoint. So there's

72
00:14:09.450 --> 00:14:26.989
Sofia Silva Berenguer: consistency can be quite broad and and some aspects of consistency that we have started working on. Documenting and exploring are the different services and features offered by the different irs! So we will start by documenting those so that we can identify and prioritize the gaps.

73
00:14:27.526 --> 00:14:29.810
Sofia Silva Berenguer: In consultation with the community.

74
00:14:30.167 --> 00:14:58.369
Sofia Silva Berenguer: Then, as I mentioned, the different Apis may be something to explore as well the mechanism to manage roas that can be through an Api or through a graphic interface, and the 5 of them are are different. So we will be exploring something along those lines as well, trying to convince some or not some hypotheses that we have. And, as I

mentioned, because we will be doing some work in the space of robustness. We will start by

75
00:14:58.770 --> 00:15:11.999
Sofia Silva Berenguer: agreeing on what are the aspects of of robustness, of the system that are worth documenting and and getting consultation with the community, trying to understand that and documenting in in a consistent way, so that it's easy to

76
00:15:12.120 --> 00:15:24.319
Sofia Silva Berenguer: identify gaps in that space as well. But of course, as I mentioned, we want to hear from the community. So if there's any other aspects of consistency that you think we should consider, I would love to

77
00:15:24.430 --> 00:15:29.369
Sofia Silva Berenguer: to hear from from the community. And I do have an email address that I would be sharing in a moment.

78
00:15:29.530 --> 00:15:31.069
Sofia Silva Berenguer: Next slide, please.

79
00:15:32.470 --> 00:15:51.179
Sofia Silva Berenguer: if you would like to know more about the Nro Rpki program. There is some information in the general website, and also in the last couple of months we have published a couple of blog articles through the fiber Iris blogs. I have included the Urls for the they are in blog

80
00:15:51.190 --> 00:15:53.340
Sofia Silva Berenguer: and next slide, please.

81
00:15:54.280 --> 00:16:21.109
Sofia Silva Berenguer: Finally, as I mentioned, we really want to hear from the technician community in particular. If you can think of any barriers or obstacles for Rpa adoption that you think we could contribute to by better coordinating and collaborating across among the Irs, I would love to hear about that. But in general, if you have any other ideas, any initiatives that

you think we should consider? Please reach out through that email address on the screen.

82
00:16:21.330 --> 00:16:24.720
Sofia Silva Berenguer: and that's it from me. I will now hand over to Brad.

83
00:16:24.830 --> 00:16:25.820
Sofia Silva Berenguer: Thank you.

84
00:16:27.900 --> 00:16:52.440
Brad Gorman: Thank you, Sophia. Thank you, everyone. April, for allowing me to speak. I've never been known to to be speaking too slowly, so I'll try to keep us on schedule. Again. My name is Brad Gorman. I work at Aaron. I'm the senior product owner, which means I go out to the community. listen to suggestions and recommendations, anything related to routing security, and then bring those suggestions and asks and recommendations back.

85
00:16:52.560 --> 00:16:59.199
Brad Gorman: And I manage the development of all of the work inside of Barron. Next slide, please.

86
00:16:59.980 --> 00:17:00.820
Brad Gorman: So

87
00:17:01.279 --> 00:17:20.940
Brad Gorman: wh what am I gonna go over? Go over a little bit of changes since last year. Things that are going on in the Us. Government that people might want to know. Go over standards, activity with with best practices and drafts, and then things that we have ahead specifically to Aaron. But certainly will help the community as a whole next slide, please.

88
00:17:23.031 --> 00:17:26.460
Brad Gorman: Last year was a year change next slide, please.

89
00:17:28.600 --> 00:17:30.759

Brad Gorman: Sophia's slide.

90
00:17:34.670 --> 00:18:00.410
Brad Gorman: next slide. Okay? So this particular chart here legends a little bit off, but it shows the the growth in organizations inside of Aaron as we signed up, or as they sign up to use Rpki services, and really 2,018 was the year that the the networking community started to accept. All of the the benefits of using Rpki, and as you move from left to right. You see how there's been a growth in

91
00:18:00.410 --> 00:18:19.430
Brad Gorman: in Aaron Usage or Aaron communities using Rbki, really, the last 2 red and yellow blocks represent a big push in getting resources under agreement, which will allow that was one of the prerequisites to using Rpki, and as so far this year we're on the same pace as 2023. Next slide, please.

92
00:18:21.171 --> 00:18:37.669
Brad Gorman: Change, was the new normal. So there was that effort to get contracts under resources under contract, which now enables more people to use Rpki. We've had a number of training and outreach activities going on in the last year and continuing through this coming year.

93
00:18:38.005 --> 00:18:53.089
Brad Gorman: We've delivered a lot of features and and done community consultations listening to and soliciting feedback from both the Aaron community and the global community, and see where we can go and deliver better services to you next slide, please.

94
00:18:54.650 --> 00:19:23.929
Brad Gorman: So last year reached, or last year reached in a milestone of IPV. 6. Announcements, heading to our on the Internet. We passed a 50, a threshold of Rpki ballot marked announcements, and on May 1st of this year, sorry. May 1st of 2024 little little mistake there. Ipv. 4. Announcements also passed a 50% threshold of being marked as Rpi ballot. So definitely, things are moving forward. Next slide, please.

95
00:19:25.686 --> 00:19:32.747

Brad Gorman: There's been a little bit of work in the standards community. A new bcp. Was released. Talk talking about

96
00:19:33.730 --> 00:19:54.980
Brad Gorman: limiting the number of of prefixes that you put into a particular roa. And again, there's also some draft work that's been going through the working group at the Itf. And one of the big things that that people have been asking for. The next knob in Rpi is the asp, the autonomous system provider authorization.

97
00:19:55.440 --> 00:20:05.729
Brad Gorman: we're still waiting on that. But it's something that people are really looking forward to, and you know, keep your your eyes and ears open, and that that should be coming hopefully later this year. Next slide, please.

98
00:20:07.872 --> 00:20:24.669
Brad Gorman: The Us. Government is really starting to take note of using Rpi as part of a national cyber security strategy that was started in early of 2023, and they talked about the importance of securing information, you know, across critical infrastructure that goes across the Internet.

99
00:20:25.008 --> 00:20:49.360
Brad Gorman: There is an increasing focus on using our Pki to do that to better secure those Bgp announcements. For the infrastructure networks. And then the Fcc. Has been active in last year with a a notice of inquiry. And then, just a few days ago, they put out a notice of proposed rule, making statement where they think that the the direction that the Us. Government

100
00:20:49.360 --> 00:20:56.569
Brad Gorman: and and Us. Organizations need to go with respect to using our Api to to protect resources

101
00:20:56.590 --> 00:20:57.820
Brad Gorman: next slide, please.

102
00:20:59.660 --> 00:21:15.509

Brad Gorman: So some of the the feature development that's coming up in Aaron this year. Going into next, we're gonna be combining and bringing the 2 Ir and Rbi routing security information databases or their database. That's closer together. It's really considered a a

103
00:21:15.510 --> 00:21:35.745
Brad Gorman: good housekeeping thing with our Bki being the the current, you know, steadfast standard, but the irr still in use, and it is an a, a routing security feature and and bringing those 2 data sets into conformity and to bringing consistent information between the 2 of them really is a good direction to go.

104
00:21:36.220 --> 00:21:52.200
Brad Gorman: our, our, our next big development effort is going to be what we call Rpka routing intelligence. It. It is a feature that other Ir customers currently are are available to them. But what it is is, we're going to be providing additional information with

105
00:21:52.520 --> 00:22:07.569
Brad Gorman: the before and after potential effects of creating rows for your resources. And then, if there are any conflicts where resources may be showing up as invalid. On the on in the Internet announcements and and giving, we will be giving recommendations on how to

106
00:22:08.291 --> 00:22:15.919
Brad Gorman: bring things up to, to what announcements are going out and and remove that invalid identification for for

107
00:22:16.241 --> 00:22:38.399
Brad Gorman: for the your announcements. We're in with the the working group that Sophia was was talking about at the Nro. We're going to be bringing together Api functionality. And the web ui, and bringing them into feature, parity, and as well anything that you wish to suggest or recommendations that you have. You know we're here to listen and to help next slide, please.

108
00:22:39.740 --> 00:22:43.280

Brad Gorman: So Rpc participation is key. It's a community effort.

109
00:22:43.540 --> 00:23:00.040
Brad Gorman: And you you with your resources, you need to sign up for Rose, and not only benefits you, but the Internet, do a greater Internet as well. These be active, become active in the standards community itf, where Rpi standards and and draft development is underway.

110
00:23:00.369 --> 00:23:25.110
Brad Gorman: Talk to your providers. If your connectivity providers are not using Rpk, push them that direction, it needs needs to happen as more and more of those providers start making decisions based on validity, data, route, origin, validation. It helps not just you, but everybody. So prepare now. So you're not surprised later whether your provider is gonna tell you that you need to do it or you're gonna sign up for new services.

111
00:23:25.915 --> 00:23:28.029
Brad Gorman: Having roas for

112
00:23:28.200 --> 00:23:33.390
Brad Gorman: covering your resources. Now, rather than later, is going to help you

113
00:23:33.500 --> 00:23:34.880
Brad Gorman: next slide, please.

114
00:23:36.403 --> 00:23:59.149
Brad Gorman: Here are the 3 ways that you can reach us at Aaron. I am the routing Security team lead, so that, you know I I always lean towards routing secure, routing dot security. aaron.net to communicate with us. But also you can reach our our registration services team at either the phone number or chat or you know other methods of communication, their email addresses as well. Next slide, please.

115
00:24:00.230 --> 00:24:04.089

Brad Gorman: There you go hopefully. You found us all up, and anybody have any questions for me or Sophia.

116
00:24:08.640 --> 00:24:20.679
Hadia Elminiawi: Thank you so much, Brad, this is Hadia again for the record. And thank you to Sophia as well. So we still have 4 min for the QAI see. Edward. So, Edward, please go ahead.

117
00:24:21.940 --> 00:24:36.129
Edward Lewis: Hi, I would say, I'm very encouraged by this. I've been tracking adoption of technologies for Rpi and also Dns sec. For much longer time. I think there's some key points here. I think that should really be drawn out one is that you turn Rpk into a service.

118
00:24:36.220 --> 00:24:37.899
Edward Lewis: not pushing technology.

119
00:24:37.950 --> 00:24:44.420
Edward Lewis: I think that's very important for many folks involved. But I looked in your details in some of the later slides that Brad had. That

120
00:24:44.440 --> 00:24:52.080
Edward Lewis: one thing you're doing is you're simplifying this. You're taking the multiple prefixes down to just one prefix per per row. You're simplifying what an operator has to deal with

121
00:24:52.651 --> 00:25:08.379
Edward Lewis: and there was something else below that that also ring true for me. Oh, the the need for operational profiles! So I think that these are to me at looking at adoption of any technology. I've I've noticed that we've had weaknesses in that area. So the question I have is, or for discussion. Here is.

122
00:25:08.380 --> 00:25:23.699
Edward Lewis: do you think the lessons learned in making our Pki successful deployment from the state it was in could be applied to other things we're

trying to secure, like Dns security, as, for example, or the other, anything else that we're trying to secure on registries and registration operations.

123
00:25:24.400 --> 00:25:43.712
Brad Gorman: Oh, that's a great question. Thanks for asking again. It the the you know it, the Rpki community it is, you know, certainly focused on that. For our Pki portions of routing security. But certainly, Dns. Sec. As it applies. You know the lessons learned and the the the best practices that we have in place.

124
00:25:44.220 --> 00:25:45.680
Brad Gorman: certainly will

125
00:25:45.690 --> 00:25:59.460
Brad Gorman: will. you know, cross the streams and and benefit one another. They have their own specific work groups in the itf, we have a meeting upcoming. And we can, you know, further, push this idea of

126
00:25:59.800 --> 00:26:18.889
Brad Gorman: you know what the the Dns community has learned and how the the routing security community has learned, you know, whether it's developing best practices or really like you said the lessons learned as deployments have gone out. That is absolutely a direction that we're going both with education and with communications.

127
00:26:23.533 --> 00:26:28.900
Hadia Elminiawi: Thank you, Brad. Sophia, do you want to? To? To further comment.

128
00:26:29.490 --> 00:26:31.510
Hadia Elminiawi: We still have 2 min.

129
00:26:32.210 --> 00:26:33.109
Hadia Elminiawi: Okay, so.

130

00:26:33.110 --> 00:26:34.060
Sofia Silva Berenguer: Any other.

131
00:26:34.060 --> 00:26:34.690
Hadia Elminiawi: Yep.

132
00:26:35.450 --> 00:26:41.049
Sofia Silva Berenguer: Oh, thanks. Yeah. I I think Brad has much more experience. I'm quite

133
00:26:41.200 --> 00:26:51.399
Sofia Silva Berenguer: Ca, kind of coming back to the technical word after a while of being focused on other topics. So I've been catching up at last few months on Rpi. But I do think that

134
00:26:52.420 --> 00:27:06.189
Sofia Silva Berenguer: in general learnings can be extrapolated and applied in different areas, and in particular with adoption of Rpi. I think what's key? Is something Brad said about preparing not to be surprised, but also that what

135
00:27:06.230 --> 00:27:22.400
Sofia Silva Berenguer: one network operator does not only for their own good, but for the whole technical community and and for securing the whole Internet. So I think that that applies to other security standards as well. Where the success of Rpki relies on

136
00:27:22.750 --> 00:27:35.899
Sofia Silva Berenguer: everyone, or mostly everyone, adopting both sides of it. So I guess that in that space there could be interesting learnings that apply to Dns. Sec. As well, or rather security protocols.

137
00:27:38.850 --> 00:28:03.689
Hadia Elminiawi: Thank you so much as Sophia, and we are at the bottom of the hour. So unless anyone else has other another question for Brad and Sophia. We can move to our panel discussion again. If you have questions,

you can put them in the Q&A pod, and also we will. We have 20 min allocated at the end of the

138
00:28:04.129 --> 00:28:22.139
Hadia Elminiawi: workshop for a Q&A so now, we move to the implementation of an is to directive, and I hand the floor to Paulina Malaysia. Center from center. she's sharing this discussion.

139
00:28:25.400 --> 00:28:54.728
Polina Malaja: Thank you, Hadia, and welcome everybody to the continuation of the role. And we'll continue with the session on the Mis. 2 implementation, and we will specifically look at the one article that will be discussing today and before setting the scene. I will also give a short presentation and give a glimpse into the data accuracy obligations that nis 2 directive has introduced.

140
00:28:55.250 --> 00:29:19.050
Polina Malaja: And yeah, after that we will hear from 3 distinguished speakers. And here on how 3 different Ccto t's are preparing for the nis to implementation and to yeah. So we will learn how how to basically translate legal requirements to the technical level and see how to address data accuracy. From the operational side.

141
00:29:19.250 --> 00:29:23.250
Polina Malaja: Without further ado. Let me also share my screen and

142
00:29:24.010 --> 00:29:25.000
Polina Malaja: give

143
00:29:25.600 --> 00:29:40.400
Polina Malaja: a brief overview of what is nis to and what is the impact of its requirements on dodd registries and registrars. I hope you'll be able to see my slides. And I assume that everything's working fine.

144
00:29:40.970 --> 00:29:42.200
Polina Malaja: So

145
00:29:42.590 --> 00:29:45.530
Polina Malaja: 1st just a few

146
00:29:46.250 --> 00:30:07.582
Polina Malaja: let's say, administrative. Oh, yeah. Points about what is the Nis to directive? And why, we are discussing it today. So as you might all have heard already. The Ns 2 is one of the latest. You cyber security legislations that is enforced already since beginning of last year.

147
00:30:08.409 --> 00:30:20.000
Polina Malaja: However, we are currently in the process of this implementation, meaning that the Directive just establishes minimum requirements, that the EU Member States need to

148
00:30:20.829 --> 00:30:45.309
Polina Malaja: follow when addressing the topic of cyber security international legislation. So they have actually, quite some time to implement the new measures and novelties that were introduced in the Nis to directive until October this year. So what is important is that it's establishes a concept of essential entities that recognizes

149
00:30:45.310 --> 00:30:49.720
Polina Malaja: the criticality of Tld infrastructure specifically.

150
00:30:49.790 --> 00:31:14.740
Polina Malaja: and it also includes a certain obligations to both Dod registries as as essential entities and registrars resellers, and privacy and proxy services as a part of the data accuracy, obligation. In Article 28. So there are also some certain penalties envisaged in case operators

151
00:31:14.740 --> 00:31:25.030
Polina Malaja: do not comply with the Nis to directive and the requirements within. So when it comes to the data, accuracy, obligation that we will look into a bit more closely. Just at the next slide.

152
00:31:25.290 --> 00:31:54.359
Polina Malaja: The penalties for noncompliance are left for Member States to decide, and these need to be effective, proportionate, and dissuasive. Another important point to note is that nis 2 has an extra tutorial effect, meaning that it's applicable to all Tl registries and entities providing domain and registration services that offer their services in the You. And the directive also gives some indication how to establish

153
00:31:54.360 --> 00:32:01.719
Polina Malaja: the fact that an operator offers this services in the EU, and you can see on the slides, for example.

154
00:32:01.840 --> 00:32:13.006
Polina Malaja: using the language and currency generally used in one or more Member States, meaning that the end user is being addressed by the operator. yeah.

155
00:32:13.680 --> 00:32:15.560
Polina Malaja: from the European perspective.

156
00:32:16.230 --> 00:32:42.139
Polina Malaja: Yeah, the operator might also or the business might also offer a possibility of ordering services in EU language and also the marketing activities are also clearly established with the EU market. So the customers and users in the you are explicitly mentioned, and for those entities that are not established in the you there is an obligation to designate a representative in the Union.

157
00:32:43.060 --> 00:32:56.610
Polina Malaja: So, moving on to the Article 28 for the purposes of our discussion, and other speakers after me will dive in how they have addressed those applications. So far. But the directing itself.

158
00:32:56.990 --> 00:33:11.309
Polina Malaja: Yeah. So it's the so called article 20, I mean. So it's Article 28, and so called data accuracy, application that it puts on do registries and

entities providing domain and registration services, meaning registrars, resellers, and privacy and proxy services.

159
00:33:11.360 --> 00:33:19.630
Polina Malaja: So first, st there's a clear, clear data set that the directive is obliging these entities to collect

160
00:33:19.970 --> 00:33:38.980
Polina Malaja: and maintain accurate and complete. This includes a domain name, data register registration, registrant name, contact email and phone number as well as email and phone number of administrative contact. If these data fields are different from the registrant data sets

161
00:33:39.500 --> 00:33:47.599
Polina Malaja: in order to keep these data sets accurate and complete, the directive mentions verification procedures that need to be put in place.

162
00:33:48.377 --> 00:34:06.569
Polina Malaja: So there are some certain clarifications in the directive itself, and it's no legislative part that gives some indication what type of verification procedures can can be put in place by the operators. So in general, there is a requirement to keep these proportionate.

163
00:34:06.570 --> 00:34:28.399
Polina Malaja: So that's in order to comply still with the overarching data protection framework. These verification procedures need to be based on best practices established within the industry and include also the developments in the electronic identification sphere both ex Sunday and expose controls are acceptable.

164
00:34:28.530 --> 00:34:44.399
Polina Malaja: and the Directive establishes as a minimum requirements or advices. The Member States to establish as a minimum as a minimum requirement, to verify at least one contact means of the registrants. So meaning either phone number or the email address.

165

00:34:45.233 --> 00:34:55.629
Polina Malaja: St registries and entities providing registration services also need to publish certain data. So basically establishes, yeah, a basic requirement to publish

166
00:34:55.639 --> 00:34:58.199
Polina Malaja: or non personal data.

167
00:34:58.950 --> 00:35:05.850
Polina Malaja: Also to include transparency on a verification procedure. So the accuracy procedures need to be

168
00:35:07.080 --> 00:35:28.529
Polina Malaja: published and pop be publicly available and in general, it offers an indication that legal persons, data, can be. Some of it can be considered a non personal data. So there is a guidance offered in the directive to publish at least a registrant name in in case it's a legal entity.

169
00:35:28.920 --> 00:35:42.800
Polina Malaja: And it's a phone number and email address. Only if it does not contain personal data. And my last points before we move on to the speakers.

170
00:35:43.120 --> 00:35:48.680
Polina Malaja: The directive is also clear that the responsibility for accuracy

171
00:35:49.181 --> 00:36:12.140
Polina Malaja: is shared between dod registries and entities providing domain and registration services. Equally so for this purposes both registries and registrars have to cooperate with each other to avoid the duplication of collecting domain and registration data, and actually, for also all the accuracy obligations under Article 28,

172
00:36:12.460 --> 00:36:38.960
Polina Malaja: and that also include providing access to legitimate access seekers when it comes to non public who is information. So yeah, for the

purposes of this final, we will go into that but with that and establishing this setting the scene, I would like to now, give floor to our speakers. Who will give yeah. As I said already in my introduction.

173
00:36:39.090 --> 00:37:06.429
Polina Malaja: a more closer look into how these legal requirements are are translated to technical level and as a 1st speaker, I would like to ask Timo with my from an Internet foundation to take the floor. And yeah, give us an introduction and an overview of how accuracy is addressed in dot e registry. So, Timo, the floor is yours, and please proceed.

174
00:37:08.290 --> 00:37:11.569
Timo Võhmar: Hello, everyone. I will be sharing my slides.

175
00:37:12.570 --> 00:37:13.330
Timo Võhmar: Connect?

176
00:37:19.990 --> 00:37:22.849
Timo Võhmar: Yeah, I hope you can see.

177
00:37:23.760 --> 00:37:24.830
Timo Võhmar: Alright.

178
00:37:24.900 --> 00:37:35.310
Timo Võhmar: So this is very exciting topic for me. I have a slide deck lasting for about an hour of presentation. I tried to really

179
00:37:36.620 --> 00:37:44.529
Timo Võhmar: crunch it up. I was able to remove like 5 min, so I just decided to speak in 5 times acceleration. So tried to

180
00:37:44.920 --> 00:37:45.719
Timo Võhmar: keep up.

181

00:37:46.800 --> 00:37:48.520
Timo Võhmar: So in case

182
00:37:48.560 --> 00:37:57.639
Timo Võhmar: we haven't met, and then I'm from the Stone winter foundation. We are not for profit foundation established in total, then for

183
00:37:57.750 --> 00:38:02.059
Timo Võhmar: managing Estonian, Ccd. Dot, d. And

184
00:38:02.590 --> 00:38:04.760
Timo Võhmar: Dns that comes with it.

185
00:38:05.930 --> 00:38:09.190
Timo Võhmar: and from the day. One

186
00:38:10.550 --> 00:38:13.680
Timo Võhmar: 1st main principle we set was to

187
00:38:14.710 --> 00:38:17.650
Timo Võhmar: identify any registrant.

188
00:38:18.200 --> 00:38:22.080
Timo Võhmar: The main idea was to keep down abuse.

189
00:38:22.670 --> 00:38:27.409
Timo Võhmar: so making making unanimous registrations close to impossible.

190
00:38:27.630 --> 00:38:43.450
Timo Võhmar: and this has worked really well for us. So in that sense we are kind of very excited to see that now this same kind of approach is sort of forced on every European registry and register.

191
00:38:44.110 --> 00:38:47.829
Timo Võhmar: So yeah, we think in the end it will be for good.

192
00:38:49.960 --> 00:38:58.799
Timo Võhmar: So how do we operate? We operate with registry register registered model. Like many or most of registries.

193
00:38:59.310 --> 00:39:09.990
Timo Võhmar: until 2,015, we had local presence requirements. So until then we could probably say that we know we knew everyone behind every registration

194
00:39:11.383 --> 00:39:18.629
Timo Võhmar: that was because of a very well established electronic identification infrastructure, Estonia

195
00:39:18.860 --> 00:39:26.019
Timo Võhmar: 2,015. We dropped local presence requirement. And now we needed them some kind of an option

196
00:39:26.690 --> 00:39:27.460
Timo Võhmar: to

197
00:39:27.910 --> 00:39:30.120
Timo Võhmar: identify everyone else as well

198
00:39:30.490 --> 00:39:32.309
Timo Võhmar: of our Europeans.

199
00:39:32.797 --> 00:39:48.300
Timo Võhmar: It does pop up at some point we were very kind of excited hope, hopeful that this will help us significantly, but in the end it and not to, because it's only available for public sector.

200
00:39:48.750 --> 00:39:51.720
Timo Võhmar: so we can't help our registrars with that.

201
00:39:52.030 --> 00:39:52.860
Timo Võhmar: So

202
00:39:53.100 --> 00:39:54.140
Timo Võhmar: we

203
00:39:54.680 --> 00:40:01.899
Timo Võhmar: kind of started started integrating these different European Eid options directly

204
00:40:02.130 --> 00:40:06.030
Timo Võhmar: and for for the countries or

205
00:40:06.070 --> 00:40:11.149
Timo Võhmar: now outside of you, and actually in inside, you as well, where people don't have

206
00:40:12.750 --> 00:40:15.330
Timo Võhmar: the strong eid option

207
00:40:16.100 --> 00:40:21.680
Timo Võhmar: implemented bank transfer based unification. So it's kind of like a

208
00:40:21.860 --> 00:40:27.489
Timo Võhmar: early stone age bank. Id type of approach. So if payment came in from

209
00:40:29.720 --> 00:40:37.013

Timo Võhmar: with with details that patch the data on registration application. For example, we considered it

210
00:40:37.580 --> 00:40:40.750
Timo Võhmar: as identified or authenticated

211
00:40:42.695 --> 00:40:46.500
Timo Võhmar: so. But pump transfers don't work really well.

212
00:40:47.900 --> 00:40:51.299
Timo Võhmar: let's say long, long distance relationships

213
00:40:51.990 --> 00:40:58.710
Timo Võhmar: where it can turn out to be very, very expensive and very time consuming. So we needed something else.

214
00:41:00.650 --> 00:41:03.890
Timo Võhmar: In our approach, we, as we

215
00:41:04.150 --> 00:41:08.590
Timo Võhmar: I've been for a long time kind of almost the only registry for

216
00:41:08.700 --> 00:41:15.796
Timo Võhmar: acquiring this strong type of identification from registrants. We have always had this kind of

217
00:41:17.720 --> 00:41:22.860
Timo Võhmar: we approach this this task so that we we should also

218
00:41:22.900 --> 00:41:31.180
Timo Võhmar: help our registrars by providing better at least list of list of acceptable options. So

219

00:41:31.290 --> 00:41:39.849
Timo Võhmar: registers don't need to go on wildcups and to try to find working solutions.

220
00:41:40.220 --> 00:41:44.310
Timo Võhmar: So yeah, we will. We have always tried out different.

221
00:41:45.238 --> 00:41:46.949
Timo Võhmar: different options out there.

222
00:41:47.000 --> 00:41:50.910
Timo Võhmar: test it, and we are very familiar with

223
00:41:52.656 --> 00:41:56.950
Timo Võhmar: with the hardship that comes with integrating with each and every one of them.

224
00:41:58.259 --> 00:42:07.259
Timo Võhmar: We have always accepted only strong identification options. So yeah, that's standard wise. It's called level of assurance high.

225
00:42:08.540 --> 00:42:17.069
Timo Võhmar: And on Epp level we have a small extension or providing identity data to the registry.

226
00:42:17.200 --> 00:42:21.960
Timo Võhmar: That is, that includes identification Id number

227
00:42:22.020 --> 00:42:25.800
Timo Võhmar: country code. And I did the type that is either

228
00:42:25.820 --> 00:42:28.450
Timo Võhmar: business sent it to your private person

229
00:42:29.840 --> 00:42:38.099
Timo Võhmar: and register needs to be able to prove how the identification was done upon request by the registry.

230
00:42:38.210 --> 00:42:39.310
Timo Võhmar: and I'll

231
00:42:39.440 --> 00:42:41.509
Timo Võhmar: talking with other registries.

232
00:42:42.130 --> 00:42:43.630
Timo Võhmar: We see that

233
00:42:45.170 --> 00:42:50.569
Timo Võhmar: different. There are multiple ways to approach this task.

234
00:42:51.250 --> 00:42:53.499
Timo Võhmar: So one way would be

235
00:42:54.664 --> 00:42:59.400
Timo Võhmar: to give kind of free hand to 30 stars. Say that. Okay.

236
00:43:00.840 --> 00:43:11.689
Timo Võhmar: you need to identify registrants in, let's say, level of assurance substantial. Yeah, it's standards meaning.

237
00:43:12.040 --> 00:43:21.469
Timo Võhmar: And it's up to the registrar to find suiting solutions and register bring in needs to be also able to kind of

238
00:43:21.760 --> 00:43:23.309
Timo Võhmar: or explain

239
00:43:23.420 --> 00:43:24.690
Timo Võhmar: why you.

240
00:43:24.700 --> 00:43:29.550
Timo Võhmar: This meets the requirements, and the idea comes from that

241
00:43:29.600 --> 00:43:32.000
Timo Võhmar: from the perspective of NS. 2,

242
00:43:32.090 --> 00:43:38.980
Timo Võhmar: register and register, both are kind of seen equally responsible for identifying

243
00:43:39.790 --> 00:43:40.840
Timo Võhmar: registrants.

244
00:43:42.300 --> 00:43:44.759
Timo Võhmar: and the other kind of approach

245
00:43:44.800 --> 00:43:49.609
Timo Võhmar: would be. The 1st one is like example would be Swedish strategy.

246
00:43:50.360 --> 00:43:57.030
Timo Võhmar: The other one is something like, let's say Denmark does. Where registry does identification.

247
00:43:57.590 --> 00:44:08.910
Timo Võhmar: So register actually doesn't need to do anything. Just point the register to the registry registry, does all the identification part, and then sends back to the register the data

248
00:44:09.950 --> 00:44:12.970

Timo Võhmar: of outcome that then, can be used to

249
00:44:12.990 --> 00:44:14.590
Timo Võhmar: for registering.

250
00:44:15.610 --> 00:44:23.809
Steve Conte - ICANN Org: You know I don't. I don't mean to interrupt. We are just want to do a slide check. We we see the slide modus operandi. Is that the correct slide that we should be looking at.

251
00:44:23.940 --> 00:44:25.309
Timo Võhmar: Well, I hope so.

252
00:44:26.960 --> 00:44:28.019
Timo Võhmar: Yeah, yeah, it sure.

253
00:44:28.020 --> 00:44:29.050
Steve Conte - ICANN Org: Okay, thank you for that.

254
00:44:29.050 --> 00:44:31.870
Timo Võhmar: I just have a lot to talk about, and

255
00:44:32.170 --> 00:44:33.590
Timo Võhmar: pretty little good. Then.

256
00:44:33.590 --> 00:44:35.040
Steve Conte - ICANN Org: Thank you. I'm sorry to interrupt.

257
00:44:35.040 --> 00:44:36.260
Timo Võhmar: Sorry for that.

258
00:44:36.420 --> 00:44:39.100
Timo Võhmar: otherwise it would be 20 slides or so

259
00:44:40.120 --> 00:44:40.980
Timo Võhmar: by Def.

260
00:44:42.470 --> 00:44:52.359
Timo Võhmar: where was I? Okay? The other option would be the registry doing the the identification. And 3rd option would be something in in between where registrars have

261
00:44:52.500 --> 00:44:58.500
Timo Võhmar: kind of an optional feature of doing it themselves, or pointing this to the registry.

262
00:44:59.602 --> 00:45:04.299
Timo Võhmar: And identifying wise our approach kind of, for

263
00:45:04.470 --> 00:45:06.109
Timo Võhmar: we see this.

264
00:45:06.200 --> 00:45:10.039
Timo Võhmar: they're perfect end result, as as

265
00:45:11.300 --> 00:45:12.889
Timo Võhmar: in the form that British

266
00:45:12.970 --> 00:45:14.000
Timo Võhmar: var

267
00:45:14.050 --> 00:45:22.410
Timo Võhmar: kind of identifies every user that approaches them, regardless of the operation they want to do, and then afterwards, of the

268
00:45:22.460 --> 00:45:24.359

Timo Võhmar: authentication they can do

269
00:45:24.550 --> 00:45:31.429
Timo Võhmar: register any any domain, at any any tnd, or to whatever other

270
00:45:34.060 --> 00:45:37.130
Timo Võhmar: task they want to do with the registrar. But

271
00:45:37.734 --> 00:45:45.019
Timo Võhmar: okay, I guess the alternative option that I heard some registries planning this kind of the signing

272
00:45:45.150 --> 00:45:47.820
Timo Võhmar: signed application approach where

273
00:45:48.370 --> 00:45:56.540
Timo Võhmar: that individual authentication is done at the end of the registration filling the registration application.

274
00:45:57.610 --> 00:46:03.694
Timo Võhmar: So there are, yeah, different different approaches to this. Just moving on quickly. So

275
00:46:04.920 --> 00:46:13.450
Timo Võhmar: how did we decide to help our registrars with this, because the bank identification wasn't kind of good enough.

276
00:46:13.470 --> 00:46:18.680
Timo Võhmar: and then as to requires identification of all the main registrants regardless of nationality.

277
00:46:19.090 --> 00:46:22.976
Timo Võhmar: So we kind of got inspired from the Idas and created

278
00:46:23.950 --> 00:46:29.180
Timo Võhmar: created similar similar kind of solution service

279
00:46:30.540 --> 00:46:34.200
Timo Võhmar: gateway basically to EU. The Ids.

280
00:46:34.550 --> 00:46:50.820
Timo Võhmar: So this kind of frees the registrars from integrating with every each and every option directly themselves, freeze them from managing the contractual agreements from ma managing the security keys.

281
00:46:51.860 --> 00:46:53.240
Timo Võhmar: and also

282
00:46:53.300 --> 00:46:56.694
Timo Võhmar: helps save some costs, because

283
00:46:57.390 --> 00:47:00.689
Timo Võhmar: especially with privately.

284
00:47:01.140 --> 00:47:07.050
Timo Võhmar: our private sector, provided the Id options like bank ids, for example, that usually come with

285
00:47:07.790 --> 00:47:08.849
Timo Võhmar: like them

286
00:47:09.080 --> 00:47:13.520
Timo Võhmar: if the price tag, if your operations are not big enough.

287
00:47:14.170 --> 00:47:14.850
Timo Võhmar: Wow.

288
00:47:15.090 --> 00:47:15.870
Timo Võhmar: so

289
00:47:16.220 --> 00:47:21.519
Timo Võhmar: kind of yeah, we hope hope to reduce this cost for for the registrars.

290
00:47:21.960 --> 00:47:24.640
Timo Võhmar: and for the rest of the world

291
00:47:25.020 --> 00:47:27.869
Timo Võhmar: decided to go with video identification.

292
00:47:29.343 --> 00:47:35.889
Timo Võhmar: For this we chose to partner up with relief. This is one of the stone and unicorns

293
00:47:36.320 --> 00:47:40.160
Timo Võhmar: that does this for banks and financial institutions.

294
00:47:40.759 --> 00:47:48.559
Timo Võhmar: So they know what they are doing. They can cover more than 10,000 different government issued ids in different

295
00:47:49.120 --> 00:47:52.340
Timo Võhmar: scripts, Latin, so like Arabic.

296
00:47:53.110 --> 00:47:54.770
Timo Võhmar: supporting

297
00:47:55.530 --> 00:47:59.140
Timo Võhmar: hundreds of different countries and nationalities and territories.

298
00:47:59.440 --> 00:48:00.940
Timo Võhmar: But there are alternatives.

299
00:48:01.010 --> 00:48:04.479
Timo Võhmar: sums up Nominat recently

300
00:48:04.600 --> 00:48:09.649
Timo Võhmar: announced that they are using meet tech, for example. So there are options out there.

301
00:48:10.320 --> 00:48:16.006
Timo Võhmar: And from the data we get from the video identification, we create

302
00:48:16.690 --> 00:48:20.400
Timo Võhmar: our own kind of eid alternate id.

303
00:48:20.780 --> 00:48:24.200
Timo Võhmar: But we then kind of protect with

304
00:48:24.430 --> 00:48:25.460
Timo Võhmar: pesky.

305
00:48:25.570 --> 00:48:26.610
Timo Võhmar: But there's a

306
00:48:28.205 --> 00:48:30.020
Timo Võhmar: fetal alliance standard.

307
00:48:30.100 --> 00:48:37.099
Timo Võhmar: I don't have time to explain this at this point, but you can check it out. All the big boys are playing with this

308
00:48:37.390 --> 00:48:38.780
Timo Võhmar: right now.

309
00:48:39.740 --> 00:48:49.910
Timo Võhmar: and the the kind of the idea of that behind the alliances to work out an alternative to usernames and passwords that is more safe and more user friendly.

310
00:48:50.160 --> 00:48:51.679
Timo Võhmar: And it kind of works. So

311
00:48:53.234 --> 00:48:57.680
Timo Võhmar: and yeah, looking into the future, we are actually also considering.

312
00:48:57.790 --> 00:49:01.490
Timo Võhmar: considering adding Google and apply the support

313
00:49:01.610 --> 00:49:03.219
Timo Võhmar: on a side.

314
00:49:03.440 --> 00:49:04.270
Timo Võhmar: And Pasqui

315
00:49:05.380 --> 00:49:13.860
Timo Võhmar: so few times I have done this presentation or this kind of presentation. I have always, I've done, Demo.

316
00:49:14.170 --> 00:49:21.919
Timo Võhmar: but I have never been able to show the video identification bit. That kind of turns out to be most interesting one

317

00:49:22.710 --> 00:49:24.500
Timo Võhmar: time being being gasped

318
00:49:24.912 --> 00:49:30.769
Timo Võhmar: the most afterwards. So I did quick to save time I did a quick recording from my mobile screen.

319
00:49:30.980 --> 00:49:33.180
Timo Võhmar: So I hope you, you can see this.

320
00:49:33.780 --> 00:49:37.510
Timo Võhmar: This is because it's my mobile screen. This is why it's kind of this

321
00:49:37.630 --> 00:49:39.590
Timo Võhmar: in this shape and the small.

322
00:49:40.090 --> 00:49:40.930
Timo Võhmar: Then

323
00:49:41.280 --> 00:49:45.020
Timo Võhmar: let's let's see. And I tried to comment and keep up with the video.

324
00:49:45.330 --> 00:49:47.180
Timo Võhmar: So this is our registrant portal.

325
00:49:47.700 --> 00:49:52.139
Timo Võhmar: You can see down there there are 2 options signing in and signing the pesky

326
00:49:53.149 --> 00:50:08.499
Timo Võhmar: let's go with a pesky in my phone. There are no Pasqui available, so I'm directed to the option to create a new identity. We have 2

options there. We have electronic ids. You can see, we have quite the long list of European ids already

327
00:50:08.540 --> 00:50:14.629
Timo Võhmar: integrated. But for this demo we go back and go with the video. Id option again

328
00:50:14.890 --> 00:50:16.219
Timo Võhmar: not already found.

329
00:50:16.880 --> 00:50:26.730
Timo Võhmar: Let me go with the Id document here and ask for my name. Last name. This is kind of a sanity check. Later on we will check this against the data we will receive from the

330
00:50:26.780 --> 00:50:30.690
Timo Võhmar: with identification step. This is very, for now

331
00:50:34.350 --> 00:50:41.120
Timo Võhmar: no, it begins. So I have to show my my document. This can be anything. Passport drives license

332
00:50:42.420 --> 00:50:43.719
Timo Võhmar: or or

333
00:50:44.220 --> 00:50:46.340
Timo Võhmar: or id card. In this instance

334
00:50:48.220 --> 00:50:52.069
Timo Võhmar: data is read directly from from the picture. This is me

335
00:50:52.860 --> 00:50:53.630
Timo Võhmar: at home

336
00:50:55.730 --> 00:50:58.010
Timo Võhmar: now, where it does, it's magic.

337
00:50:58.500 --> 00:50:59.849
Timo Võhmar: Everything checks out

338
00:51:01.660 --> 00:51:04.260
Timo Võhmar: data sent to us. We are doing our magic now.

339
00:51:04.570 --> 00:51:06.239
Timo Võhmar: I'll additional checks.

340
00:51:08.620 --> 00:51:16.510
Timo Võhmar: and the pesky is generated because it will worked out and saved to my my phone and protected with my biometric data.

341
00:51:21.080 --> 00:51:28.230
Timo Võhmar: And here we go. This is our additional portal, and these are my my domains. And just to show how this will look next time.

342
00:51:28.390 --> 00:51:33.420
Timo Võhmar: When user approaches this service, or any other service that has the id enabled

343
00:51:34.710 --> 00:51:39.830
Timo Võhmar: key is found, I enable access with my fingerprint in this instance.

344
00:51:41.690 --> 00:51:42.910
Timo Võhmar: and we got back in

345
00:51:43.100 --> 00:51:45.170
Timo Võhmar: a very easy, safe fund

346
00:51:45.500 --> 00:51:46.580
Timo Võhmar: convenient.

347
00:51:51.100 --> 00:51:55.260
Timo Võhmar: Okay? And this is a small, quick schematics. What's going on.

348
00:51:55.360 --> 00:51:58.459
Timo Võhmar: So we are creating new Id

349
00:51:58.960 --> 00:52:00.290
Timo Võhmar: we have.

350
00:52:00.730 --> 00:52:02.349
Timo Võhmar: we can take in

351
00:52:02.750 --> 00:52:07.400
Timo Võhmar: existing the Ids bank Ids government provided ids, or

352
00:52:07.640 --> 00:52:09.640
Timo Võhmar: or the video Id option.

353
00:52:10.080 --> 00:52:10.800
Timo Võhmar: And

354
00:52:12.241 --> 00:52:17.060
Timo Võhmar: we product protected with multi-factor authentication using pass keys.

355
00:52:17.230 --> 00:52:25.119
Timo Võhmar: The It service itself is a web app. So nothing needs to be installed by the end user to their phone, to their computer.

356
00:52:26.340 --> 00:52:31.909
Timo Võhmar: It's based on open id connect protocol and relies on both those standard.

357
00:52:35.730 --> 00:52:42.919
Timo Võhmar: Okay? And this is the output that we sent back for the Id service sends back to the register.

358
00:52:43.260 --> 00:52:44.830
Timo Võhmar: Acr

359
00:52:44.890 --> 00:52:48.000
Timo Võhmar: is kind of the level of assurance. So

360
00:52:48.290 --> 00:52:54.979
Timo Võhmar: the strength of the identification that was used to create this id, we have

361
00:52:55.410 --> 00:52:56.400
Timo Võhmar: timestamp

362
00:52:56.840 --> 00:52:58.330
Timo Võhmar: of the

363
00:52:58.370 --> 00:53:00.060
Timo Võhmar: authentication operation.

364
00:53:00.840 --> 00:53:05.600
Timo Võhmar: We have information about the authentication type. This is

365
00:53:06.290 --> 00:53:11.280
Timo Võhmar: the Id or the method that was id that was used to create

366
00:53:11.570 --> 00:53:12.680
Timo Võhmar: and the

367
00:53:13.360 --> 00:53:14.420
Timo Võhmar: identity.

368
00:53:14.680 --> 00:53:17.920
Timo Võhmar: So this can be passport. This can in this instance.

369
00:53:18.140 --> 00:53:19.270
Timo Võhmar: smart. Id.

370
00:53:19.980 --> 00:53:29.380
Timo Võhmar: this is another yeah. Id option date of birth. We have name, family name, 1st name, and the sub is the personal id of the person.

371
00:53:32.080 --> 00:53:37.060
Timo Võhmar: and this is it. I hope I'm in time lost the check of time.

372
00:53:37.360 --> 00:53:38.770
Timo Võhmar: Somewhere in between. There.

373
00:53:43.370 --> 00:53:59.943
Polina Malaja: Thank you, Timo. Thank you very much for this overview. So I see that we received already some questions. But we will take them in the end of the session. After all, speakers have a chance to present their solutions, so some of them might be addressed, perhaps. After all,

374
00:54:00.250 --> 00:54:17.859
Polina Malaja: speakers have spoken. So now I would like to move on to Alex. May offer from nick it, and yeah, to present his work on the Evp. And dot 80 solutions to data accuracy, application under Article 28, Alex. The floor is yours.

375
00:54:17.860 --> 00:54:18.710
Polina Malaja: Go ahead.

376
00:54:18.710 --> 00:54:21.427
Alexander Mayrhofer: Thank you, Paulina. Thank you. Everybody.

377
00:54:22.020 --> 00:54:28.509
Alexander Mayrhofer: thanks for giving me that time to actually present. What we have been working for in is 2

378
00:54:29.690 --> 00:54:54.809
Alexander Mayrhofer: so our our approach is that we would actually create an Epp extension for nis 2. And please understand, because what we are presenting here is like draft work that is still in discussion, but I also wanted to share it reasonably early looking at October. It's not that early, but anyways and and use that opportunity to garner feedback from the community.

379
00:54:55.150 --> 00:54:56.920
Alexander Mayrhofer: So next slide, please.

380
00:54:58.610 --> 00:55:14.570
Alexander Mayrhofer: yeah. What I'm gonna speak about it. Let me maybe briefly introduce myself. My name is Alex Mayor Hoffer. I work for.it, which is the Austrian country code Cctld. And I'm the team leader of the research and development team. And one of our

381
00:55:14.690 --> 00:55:20.539
Alexander Mayrhofer: tasks is to actually look at the Nis 2 implementation options for our Cct.

382
00:55:20.640 --> 00:55:26.004
Alexander Mayrhofer: so I'll briefly talk about.id, what what our size and what our structure is.

383
00:55:26.550 --> 00:55:36.510
Alexander Mayrhofer: we go over the processes on a very high level, on how we intend to cover the Nis. 2. Article 28 requirements.

384
00:55:36.710 --> 00:55:45.830
Alexander Mayrhofer: and will subsequently present the idea of a verification report and provide you with some actual

385
00:55:46.180 --> 00:55:48.580
Alexander Mayrhofer: Epp frames. How we intend

386
00:55:48.690 --> 00:55:52.219
Alexander Mayrhofer: that would work out in the near future. So next slide, please.

387
00:55:53.730 --> 00:55:57.240
Alexander Mayrhofer: Thank you. So thought it.

388
00:55:57.280 --> 00:56:01.529
Alexander Mayrhofer: Dot 80 exists since I think 1989.

389
00:56:01.650 --> 00:56:03.549
Alexander Mayrhofer: And as of

390
00:56:03.560 --> 00:56:13.089
Alexander Mayrhofer: as as we speak, we have about 1.5 million active registrations. We said, really excellent retention rate of about 90%. So that's something that we were really proud of.

391
00:56:13.130 --> 00:56:15.370
Alexander Mayrhofer: so our customers tend to stick around.

392
00:56:15.600 --> 00:56:23.150

Alexander Mayrhofer: We were founded in 1,997, and have been operating the Dod since that time.

393
00:56:23.270 --> 00:56:37.699
Alexander Mayrhofer: and currently we have about 450 registrars of various different sizes, different structure from very small ones, with a couple of 100 domain names to very peak ones with 6 digit domains under management.

394
00:56:38.950 --> 00:56:42.600
Alexander Mayrhofer: our NIS, 2, implementation is currently ongoing.

395
00:56:42.610 --> 00:56:45.269
Alexander Mayrhofer: And the the process that we

396
00:56:45.490 --> 00:56:48.330
Alexander Mayrhofer: created together with our registrars.

397
00:56:48.340 --> 00:56:49.610
Alexander Mayrhofer: is that

398
00:56:49.630 --> 00:56:51.779
Alexander Mayrhofer: the registry we essentially

399
00:56:52.380 --> 00:56:55.970
Alexander Mayrhofer: select domains for verification. If we believe

400
00:56:56.170 --> 00:56:59.719
Alexander Mayrhofer: that the data that comes with the registration

401
00:57:01.450 --> 00:57:05.140
Alexander Mayrhofer: might require verification. Let me put it that way, and

402
00:57:05.310 --> 00:57:10.689

Alexander Mayrhofer: after that the registra will be tasked with verifying the owner information

403
00:57:10.710 --> 00:57:13.139
Alexander Mayrhofer: and provide info to the registry.

404
00:57:15.450 --> 00:57:16.350
Alexander Mayrhofer: to

405
00:57:16.490 --> 00:57:22.220
Alexander Mayrhofer: keep the domain name essentially, but but more on that on the on the next slide. So next one, please.

406
00:57:25.160 --> 00:57:45.660
Alexander Mayrhofer: Yes. So this is a boilerplate draft. Thank you. So this is a very high, level view of our of our process that I call the happy past. So I'm sorry for my handwriting, but I'm going to read it for you. So what happens is that there's a domain name

407
00:57:45.810 --> 00:57:54.590
Alexander Mayrhofer: potentially like a recent registration. Let me put it that way. And so the registry would do some magic. And if the metric says that

408
00:57:54.850 --> 00:58:01.599
Alexander Mayrhofer: there are indications that the address information provided, or the name or the phone number or the email address

409
00:58:01.860 --> 00:58:17.359
Alexander Mayrhofer: might be incorrect, then the register will select the domain for verification, and the registrar would at that point in time receive a notification that tells them verification required, and the register will then

410
00:58:17.580 --> 00:58:18.550
Alexander Mayrhofer: either

411
00:58:18.870 --> 00:58:28.449
Alexander Mayrhofer: look into his customer database, for example, if he's also providing Dsa services for that consumer, he might have a reasonable good customer record.

412
00:58:28.968 --> 00:58:31.120
Alexander Mayrhofer: If not, you might need to

413
00:58:31.300 --> 00:58:33.939
Alexander Mayrhofer: contact the customer in the 1st place.

414
00:58:34.010 --> 00:58:43.560
Alexander Mayrhofer: and after that, in that happy pass. We assume that the registrar provides that information about that verification

415
00:58:43.730 --> 00:58:48.790
Alexander Mayrhofer: to the registry at which we believe that everything is correct, and to the main

416
00:58:49.010 --> 00:58:52.126
Alexander Mayrhofer: we happily live ever after.

417
00:58:52.980 --> 00:58:57.310
Alexander Mayrhofer: There's a timeout for this 1st step of the process of about 21 days.

418
00:58:57.430 --> 00:59:06.990
Alexander Mayrhofer: and please bear in mind that this is actually a draft process. So we are presenting it to our own registrars actually by tomorrow. So you get sort of like a sneak preview.

419
00:59:08.430 --> 00:59:09.800
Alexander Mayrhofer: thank you. Next one.

420
00:59:11.420 --> 00:59:14.910
Alexander Mayrhofer: So what I call the death row pause. So

421
00:59:15.130 --> 00:59:17.620
Alexander Mayrhofer: if there's something wrong with it.

422
00:59:17.670 --> 00:59:29.760
Alexander Mayrhofer: domain Holder information that doesn't fulfill the requirements for Article 28, or we believe it to be, then there will be like a longer process. We have seen already. The 1st part at the very left is like selected for verification

423
00:59:30.308 --> 00:59:38.879
Alexander Mayrhofer: and after that the register receives a notification about that. If the register doesn't react in the 1st 14 days.

424
00:59:38.940 --> 00:59:48.480
Alexander Mayrhofer: that's not not on the screen. Then there will be more notifications that we call last morning to the registra, and in that case also to the domain name holder.

425
00:59:48.760 --> 00:59:56.740
Alexander Mayrhofer: So essentially, we are giving the registrar 14 days to work it out by themselves before we approach the registrant. Directly.

426
00:59:57.790 --> 01:00:04.330
Alexander Mayrhofer: this happens 14 days after. If the registrar doesn't react within 21 days, or the registrar

427
01:00:04.641 --> 01:00:09.710
Alexander Mayrhofer: then we put the domain server hold. That means that it will be taken out of the Dns.

428
01:00:10.020 --> 01:00:15.350

Alexander Mayrhofer: And at this point in time there will obviously be more notifications about this activity

429
01:00:15.400 --> 01:00:18.629
Alexander Mayrhofer: to post the domain name holder, and again the register

430
01:00:20.350 --> 01:00:26.010
Alexander Mayrhofer: if the registrant and the registrar still do not react in those. In that period of time

431
01:00:26.270 --> 01:00:40.770
Alexander Mayrhofer: there will be 30 days until we finally cancel the contract with the customer. So we essentially like cancel the contract disposal, for that specific domain is the registrar, and with the registrant.

432
01:00:40.950 --> 01:00:43.229
Alexander Mayrhofer: and the domain goes in to cool down

433
01:00:43.460 --> 01:00:52.430
Alexander Mayrhofer: at this point. There will also be notifications, of course. So you can see actually, if you go this through this process, you have like a ton of notification

434
01:00:52.590 --> 01:01:06.780
Alexander Mayrhofer: in your mailbox or message queue, and if the registrant doesn't react to the registrar after 30 about 2 months, sorry! About 2 months in that Cooldown, the domain name is being purged and becomes available for re-registration

435
01:01:07.690 --> 01:01:08.560
Alexander Mayrhofer: next one.

436
01:01:10.240 --> 01:01:39.519

Alexander Mayrhofer: So we thought a little bit about how we would actually implement this on the data level. And we we came up that some be something that we call the verification report. So if you look at this very closely, the verification data is actually independent from the attributes of the contact itself. So it's actually metadata that tells. Yes, this contact data is actually correct. And therefore we believe that it shouldn't stick directly on the contact.

437
01:01:40.680 --> 01:01:41.660
Alexander Mayrhofer: And

438
01:01:41.690 --> 01:01:46.566
Alexander Mayrhofer: that made us motivated us to to think about that idea.

439
01:01:47.270 --> 01:02:08.939
Alexander Mayrhofer: And if you look at it very closely. What the registry receives is actually not the properties of the contact itself, but rather like a report of a verification. So it's a report of an activity, and it's also not up to the registrar to decide what the status is with that contact, but rather for the registry

440
01:02:09.130 --> 01:02:13.229
Alexander Mayrhofer: to decide if the information contained in a verification report

441
01:02:13.360 --> 01:02:18.970
Alexander Mayrhofer: constitutes enough information to to like change the status of the contact object.

442
01:02:19.290 --> 01:02:28.850
Alexander Mayrhofer: So out of these ideas and this way of thinking. We called. We called the the existing structure a verification report.

443
01:02:29.120 --> 01:02:31.210
Alexander Mayrhofer: and if you're into Epp.

444
01:02:31.450 --> 01:02:46.869
Alexander Mayrhofer: which I suppose some of us are unfortunately, or fortunately. Then you might have seen something similar, which is the restore report that you can see in Rfc. 3, 9, 15, which Gtd. Registries are very familiar, I believe.

445
01:02:49.740 --> 01:02:50.949
Alexander Mayrhofer: next one, please.

446
01:02:54.300 --> 01:03:03.659
Alexander Mayrhofer: So what at this point in time do we actually believe we should receive from the registrar? And we actually

447
01:03:04.180 --> 01:03:06.780
Alexander Mayrhofer: don't want to receive the data itself.

448
01:03:06.930 --> 01:03:27.270
Alexander Mayrhofer: but you are the only one to receive. A couple of metadata fields about that verification activity, and the 1st one is obviously the result. So the most obvious one is like success. So the registrar has successfully verified that registrant and sends in that indication A timestamp.

449
01:03:27.280 --> 01:03:32.100
Alexander Mayrhofer: which is state time of completion of the verification process. Not the beginning of it.

450
01:03:32.589 --> 01:03:45.899
Alexander Mayrhofer: A method. It's still unclear whether this is going to be an identifier, or it's going to be just a description of the method. So it could be something like passport, copy or utility B, or whatever

451
01:03:46.454 --> 01:03:53.150
Alexander Mayrhofer: the other one is going to be a reference number. That's a reference number on the side of the entity that actually

452
01:03:53.180 --> 01:03:54.870
Alexander Mayrhofer: perform to verification

453
01:03:56.250 --> 01:03:57.390
Alexander Mayrhofer: and

454
01:03:57.430 --> 01:04:27.039
Alexander Mayrhofer: what we call agent right now. That is the name of the entity that performed that verification. Why are those 2 fields in? Because we reserved the right in our legal documents to actually audit the registrar. If we believe that the verification that the registrar has indicated was successful wasn't successful, then we would approach the register and say, Hey, agent, y told you in reference number Y, that this was successful, and please provide us with documentation to prove this

455
01:04:27.470 --> 01:04:36.590
Alexander Mayrhofer: so reasonable. Simple, no signatures, no complex data structures, just like a set of fields that relate to the to the actual activity

456
01:04:36.800 --> 01:04:37.710
Alexander Mayrhofer: next one.

457
01:04:39.077 --> 01:04:40.509
Alexander Mayrhofer: Yes. And we

458
01:04:40.530 --> 01:04:49.770
Alexander Mayrhofer: need to put this into an Epp extension. So we're going to add something that we call the verification report into Epp, and we have corresponding status values next one

459
01:04:51.930 --> 01:04:52.940
Alexander Mayrhofer: so

460
01:04:53.110 --> 01:05:16.419

Alexander Mayrhofer: just very briefly, we chose a so-called command response extension to Epp. If you have been to extending Epp, you know that there are 3 different kind of ways to actually extend Epp, and the common response extension is the simplest. And therefore we also preferred that one, because we believe that the whole industry is going to be PC news. Other things.

461
01:05:16.590 --> 01:05:28.750
Alexander Mayrhofer: and the extension that we propose effect 3, 4 commands, contact update contact, create contact, info and domain info, and it also extends a couple of notifications that we send out

462
01:05:29.110 --> 01:05:30.050
Alexander Mayrhofer: next one.

463
01:05:31.970 --> 01:05:44.999
Alexander Mayrhofer: And yeah, here's a practical example how the contact update might look like. So if you look at the Epp's frame itself, it essentially contains an empty contact change element.

464
01:05:45.160 --> 01:06:05.220
Alexander Mayrhofer: and the important stuff is in the in the extension below which says verification report. The result of the verification was success. Verification happened actually 21 years in the past. So this is an interesting question, how old can a verification be. But this would be registry policy.

465
01:06:05.290 --> 01:06:15.300
Alexander Mayrhofer: And then the message was passport copy. And there's a certain reference number on the site of the agent that provided the certification. And that's it.

466
01:06:15.933 --> 01:06:28.329
Alexander Mayrhofer: This will be possible on a contact update command, and also at the same time, you create a contact so essentially both of those commands will look pretty much identical

467
01:06:28.850 --> 01:06:29.720
Alexander Mayrhofer: next one.

468
01:06:31.430 --> 01:06:32.450
Alexander Mayrhofer: So

469
01:06:32.510 --> 01:06:33.899
Alexander Mayrhofer: contact info

470
01:06:34.010 --> 01:06:42.510
Alexander Mayrhofer: essentially what we do is during the contact info, we would mirror the like latest verification report that we received.

471
01:06:42.570 --> 01:06:59.139
Alexander Mayrhofer: So it's like a stack of paper. You only see the latest one. And in addition to the fields that were actually submitted to the registry, there would be another 2 fields registry generated that would indicate the timestamp at which this verification was submitted to the registry

472
01:06:59.140 --> 01:07:13.010
Alexander Mayrhofer: and the client. Id of the client. Yeah. Who that submitted that verification, because the verification will actually survive a transfer of a contact to a different registrar.

473
01:07:14.600 --> 01:07:15.820
Alexander Mayrhofer: Next one, please.

474
01:07:18.100 --> 01:07:30.820
Alexander Mayrhofer: An example for the domain information. What do we need to put in here? We need to add a couple of status values that are independent of the currently existing domain status values, and the most prominent one that will be

475

01:07:30.830 --> 01:07:39.139
Alexander Mayrhofer: present when a domain name has been selected for verification is that we put a pending verification status on top of it on on that domain.

476
01:07:39.230 --> 01:07:43.210
Alexander Mayrhofer: and it also has an action on till date timestamp.

477
01:07:43.310 --> 01:07:49.989
Alexander Mayrhofer: which indicates on, up to which point in time the registrar can actually perform verification

478
01:07:51.420 --> 01:07:52.309
Alexander Mayrhofer: next one.

479
01:07:54.500 --> 01:08:02.349
Alexander Mayrhofer: And so next steps in this. This is the 1st public presentation of our work. We will

480
01:08:02.600 --> 01:08:09.479
Alexander Mayrhofer: present this work to our own registrars in the next couple of days more precisely tomorrow and the day after tomorrow in English.

481
01:08:09.750 --> 01:08:21.410
Alexander Mayrhofer: and we will do refinement of the the Id and the extensions. What's especially challenging is, of course, some multi domains scenarios where one registrant has multiple domains.

482
01:08:22.158 --> 01:08:25.369
Alexander Mayrhofer: Notifications. I haven't shown any of these.

483
01:08:25.520 --> 01:08:27.150
Alexander Mayrhofer: These will be fine tuned.

484
01:08:27.260 --> 01:08:29.140
Alexander Mayrhofer: and we will create a schema.

485
01:08:29.359 --> 01:08:35.729
Alexander Mayrhofer: And at the same time we are doing specification for the actual policy of the registry that is independent of the extension

486
01:08:35.990 --> 01:08:38.070
Alexander Mayrhofer: and implement this.

487
01:08:38.550 --> 01:08:44.889
Alexander Mayrhofer: And if resources and interest permits, we will probably put this into an Internet draft and submit it to the Idf.

488
01:08:46.410 --> 01:08:54.770
Alexander Mayrhofer: That's it. I think that is my last slide. Yes. So here's a brief summary. We are 1.5 million Cct. From Europe.

489
01:08:56.310 --> 01:09:01.320
Alexander Mayrhofer: our process is registry request, certification. Registrar provides verification info.

490
01:09:01.399 --> 01:09:07.630
Alexander Mayrhofer: We do something that looks like Rsc. 3, 9, 15, restore report, and that's called Verification report

491
01:09:07.850 --> 01:09:13.189
Alexander Mayrhofer: and the extension will affect the contact. Create contact, update contact infant info.

492
01:09:13.930 --> 01:09:15.700
Alexander Mayrhofer: That's it. Thank you.

493

01:09:17.960 --> 01:09:42.920
Polina Malaja: Thank you, Alex, for a very interesting presentation. So we are a little bit running behind the time. But with, gracious help from Heidi and Steve will extend a little bit the time for the panel discussion, so that we can take the questions from the QA pod. So without further ado, I would like to give now the floor to Michael Palace, who will give a presentation or take us through Pavel's presentation, so unfortunately.

494
01:09:42.920 --> 01:09:54.980
Polina Malaja: cannot be with us today. But Michael has very kindly agreed to take a 3 presentation and present Phenix view on Article 28. Implementation. So, Michael, the floor is yours. Thank you.

495
01:09:54.980 --> 01:10:18.430
Michael Palage: Thank you, Paulina, and I will try to catch up and get us back on time. So one of the things I would like to tell everyone Tom Keller, who's the Executive board member of D Nick? Yeah. Tom gave a presentation at Ican 79 during the alac plenary. About this implementation as well. So there is a again. Another additional resource

496
01:10:18.890 --> 01:10:20.510
Michael Palage: next slide, please.

497
01:10:22.349 --> 01:10:26.449
Michael Palage: Paulina, you have already discussed this. The background. Next slide.

498
01:10:28.530 --> 01:10:29.929
Michael Palage: Next slide.

499
01:10:31.409 --> 01:10:56.189
Michael Palage: Yes. So one of the things that I think is very unique about Dnick's approach to N is 2 is when they realized they didn't know what to do. What they deferred to was to actually create a working group with the registrars and some of the principles that drove the work of Dick is that they were not only looking for a solution that would be able to be implemented

500
01:10:56.664 --> 01:11:05.200
Michael Palage: by November, when Nis 2 will go into effect, but they also wanted to provide flexibility, to adjust

501
01:11:05.200 --> 01:11:13.940
Michael Palage: and be able to change in the future and potentially provide for the potential reusability of verification.

502
01:11:13.940 --> 01:11:21.650
Michael Palage: So again, very not short focus, but also looking over the horizon. Next slide, please.

503
01:11:23.279 --> 01:11:44.870
Michael Palage: So one of the main points. That was driven home to denic in its consultation with its registrar members. Is the idea that in a number of cases, a large percentage of registrar registrants will have registrations and multiple Tlds.

504
01:11:44.870 --> 01:11:59.600
Michael Palage: So this fact of how registrars and their registrants would go about providing enhanced verification across an a number of Tld's was was a driving consideration of their work. Next slide, please.

505
01:12:02.342 --> 01:12:04.389
Michael Palage: We can go to the next slide.

506
01:12:05.800 --> 01:12:30.269
Michael Palage: So what we have here, and I think we we heard this Alex. Was talking about this registries. A number of the European regist European cctld registries have taken one of 2 approaches to Nis. There are some that are more focused in on the registry doing the verification, or others that want to defer to the registrar.

507
01:12:30.270 --> 01:12:42.130

Michael Palage: So what you see here online is an email from the.dk registry sending out a verification request to the domain name registrant next slide.

508
01:12:42.940 --> 01:13:08.489
Michael Palage: So one of the problems that the working group within d Nic result focused on, particularly in the short term, was the burden that this created for all all parties involved, and the, if you will, miserable ux ui experience and the friction that it potentially would create, as well as the additional cost that might be imposed next slide, please.

509
01:13:10.257 --> 01:13:15.969
Michael Palage: So the question was, what do we do? How how do we solve this problem? Next slide, please?

510
01:13:16.922 --> 01:13:40.000
Michael Palage: So one of the things, particularly those from Europe. Is Eid will save us but as Pavel notes here, not yet. I'm I'm in fact, I literally just attended a presentation by the German Federal Federal Ministry of Interior and Communication talking about eitis 2 2 0

511
01:13:40.000 --> 01:13:48.678
Michael Palage: here today in Berlin. But as Pavel says, this is still a couple of years down the line. So in the immediate

512
01:13:49.970 --> 01:14:00.329
Michael Palage: in the immediate future, particularly with this implementation being required by October. What was Dnick's approach to solve this problem next slide?

513
01:14:02.570 --> 01:14:28.659
Michael Palage: So one of the things that is very key towards Dnick's approach is they wanted to rely on the extensive verification process that it's existing. Registrar members have, instead of coming up with a 1 size, fits all approach. Dnick wanted to leverage the plethora of verification. It methods. That it red. It's registrar network has next slide, please.

514

01:14:30.040 --> 01:14:31.190
Michael Palage: Next slide

515
01:14:34.460 --> 01:14:36.889
Michael Palage: If we can next slide

516
01:14:37.320 --> 01:14:38.869
Michael Palage: next slide.

517
01:14:39.475 --> 01:15:06.580
Michael Palage: Yes, here. So what you see in this slide is is basically the challenge of how do 2 registries go about federating? Registrant contact details among 2 registries that may have different verification requirements. So this was the challenge that the the d Nic working group was addressing next slide, please.

518
01:15:08.288 --> 01:15:33.691
Michael Palage: So one of the this. These are some of the if you will. High level points. That came from this working group, and the current approach that D Nick is taking towards implementing and meeting the N is 2 requirements that will go into effect later this year. Their focus was to have the regist was to have the registrar do the verification

519
01:15:34.060 --> 01:15:50.989
Michael Palage: much like Alex mentioned. Dick will be doing a a querying, and we'll be identifying 2, basically 3 types of domain names. There is low risk, high risk, and then very high risk

520
01:15:51.421 --> 01:16:05.229
Michael Palage: for very high risk. Domain names. Those names will be blocked from resolution. High risk will be permitted to resolve for 2 weeks, but we'll have to undergo a verification request.

521
01:16:05.687 --> 01:16:21.700

Michael Palage: One of the things that is very key about the d Nic approach is how they intend to require the registrar to identify in metadata how the verification was in fact, undertaken.

522
01:16:21.700 --> 01:16:23.220
Michael Palage: Next slide, please.

523
01:16:25.993 --> 01:16:51.140
Michael Palage: And again what what they were looking to do here is again leverage some of the existing processes that were already in the marketplace, and and again I would refer everyone to Tom Keller's presentation from I can. 69 where he went into greater detail regarding the traffic light protocol towards the registration process next slide.

524
01:16:52.537 --> 01:17:15.742
Michael Palage: One of the things that I think is key. And I I really do applaud of the work that D Nick is doing here is they are. Look! They are looking at a number of initiatives that are being done in standards, body particularly the open identity foundation about how there is the potential to do this, and just a a quick other note,

525
01:17:16.340 --> 01:17:39.526
Michael Palage: with some of the other registries that have done work. Czi Nick, actually worked with a number of other European Cct registries in the Reggie id program which was funded by the Commission to show about the Federation of data between registries. And with that just mindful of time. I want to leave enough time for questions, so

526
01:17:39.900 --> 01:17:56.460
Michael Palage: I will tend to end it there. And if anyone does have any specific questions regarding the d nic implementation please forward them to us, or and we will make sure that they are directed to Pavel so that he could answer it. So back to you, Paulina.

527
01:17:58.060 --> 01:18:17.772
Polina Malaja: Thank you, Michael, and thank you for yes, keeping keeping a good track of time with the presentation. So we have a little bit a few more

minutes to address some of the questions that I received in the QA. Pod. So, in the interest of time, I will just direct a few of them directly to our speakers. So meaning Timo and Alexand A. Alex.

528
01:18:18.050 --> 01:18:39.439
Polina Malaja: Because yeah, for Pavel, I assume we will just direct question directly to him. So and yeah, we will take them as as much as we can in 5 min. So 1st a question to Timo. From Alexander. Why did you decide to use the level of a authentication substantial?

529
01:18:39.440 --> 01:18:50.440
Polina Malaja: And should it be the level of often the authentication low enough to identify the registrant. So that's the 1st question to you, team of if you can. Give us a quick answer in that.

530
01:18:51.260 --> 01:18:56.470
Timo Võhmar: Well, in our case. We have always aim that level high. Actually.

531
01:18:56.530 --> 01:19:01.219
Timo Võhmar: so coming down to level substantially is already kind of step back

532
01:19:01.260 --> 01:19:09.019
Timo Võhmar: in in that sense. But we feel that the the requirements for the level low is

533
01:19:10.110 --> 01:19:11.730
Timo Võhmar: kind of pointless.

534
01:19:11.840 --> 01:19:13.150
Timo Võhmar: To be frank.

535
01:19:13.940 --> 01:19:17.200
Timo Võhmar: they they don't have really.

536
01:19:17.960 --> 01:19:19.410
Timo Võhmar: I don't know. Then

537
01:19:19.440 --> 01:19:23.601
Timo Võhmar: I don't feel that the that person is actually kind of

538
01:19:24.290 --> 01:19:28.429
Timo Võhmar: identified or verified behind

539
01:19:30.180 --> 01:19:30.930
Timo Võhmar: operation.

540
01:19:31.370 --> 01:19:42.660
Timo Võhmar: So yeah, we we decided to go with substantial. We think this is kind of simple enough task, and at the end secure enough to

541
01:19:42.730 --> 01:19:47.980
Timo Võhmar: keep the zone safe, so to say. But we are open for

542
01:19:48.350 --> 01:19:51.229
Timo Võhmar: other suggestions, and and

543
01:19:51.270 --> 01:19:53.899
Timo Võhmar: ready to change our mind if we

544
01:19:53.920 --> 01:19:55.769
Timo Võhmar: here good enough arguments.

545
01:19:58.260 --> 01:20:09.421
Polina Malaja: Thank you, Timo. Very clear. And so, yeah, I think from my side again, just at at the higher levels. Give more assurance, and primarily also to the supervising authorities.

546
01:20:10.291 --> 01:20:19.199
Polina Malaja: And another question for you, Tima, from your team. Regarding pass keys. Does your system support adding more than one per person?

547
01:20:19.620 --> 01:20:20.730
Polina Malaja: The question.

548
01:20:21.580 --> 01:20:23.020
Timo Võhmar: Yes.

549
01:20:23.340 --> 01:20:25.370
Timo Võhmar: answer. Short answer is yes.

550
01:20:29.760 --> 01:20:44.330
Polina Malaja: Thank you for a short answer. So then I will move on to the questions to Alex. So 1st from Jim. So Alex. It's not clear how the registry would determine what domains require verification.

551
01:20:44.410 --> 01:20:51.050
Polina Malaja: What percentage of the domains do you anticipate the registry request for the verification information.

552
01:20:52.170 --> 01:20:53.677
Alexander Mayrhofer: Yes, thank you.

553
01:20:54.300 --> 01:21:03.529
Alexander Mayrhofer: our preliminary data on currently existing registrations indicates we would send about 1% to 2% of the registrations into verification.

554
01:21:04.790 --> 01:21:08.180

Alexander Mayrhofer: That's a new registration. So I haven't looked at all of the old ones.

555
01:21:10.180 --> 01:21:28.759
Polina Malaja: Thank you, Alex. Also for a short answer, and another question to you from Daniela. And she's asking if you verify the registrants upon the up, the submission of the application. And whether do you request, approve of Id

556
01:21:28.910 --> 01:21:32.809
Polina Malaja: and other identification documents? I assume.

557
01:21:34.594 --> 01:21:48.169
Alexander Mayrhofer: We believe that we let the registrar decide on how they would properly fulfill the requirements, because it's actually allotted affects both the registry and the registrar.

558
01:21:48.340 --> 01:21:49.235
Alexander Mayrhofer: So

559
01:21:50.290 --> 01:21:52.379
Alexander Mayrhofer: We don't prescribe any missiles

560
01:21:52.690 --> 01:22:01.440
Alexander Mayrhofer: we might indicate what methods we are going to use as a registrar of last resort. But we are not prescribing

561
01:22:02.240 --> 01:22:06.639
Alexander Mayrhofer: whatever method they would use, nor do we actually require that they communicate to us

562
01:22:06.740 --> 01:22:11.120
Alexander Mayrhofer: any kind of information about the actual verification?

563

01:22:12.300 --> 01:22:14.879
Alexander Mayrhofer: Did that cover the question?

564
01:22:15.280 --> 01:22:16.080
Alexander Mayrhofer: Sort of.

565
01:22:18.640 --> 01:22:19.390
Polina Malaja: Yes.

566
01:22:19.600 --> 01:22:20.380
Polina Malaja: yes.

567
01:22:21.375 --> 01:22:34.009
Polina Malaja: So no prescription of verification. methods. And yeah, and whether you verify at the registrant when the application is submitted. So I think, yeah.

568
01:22:34.330 --> 01:22:40.510
Alexander Mayrhofer: We don't do applications. So the registration goes into the Dns immediately.

569
01:22:40.580 --> 01:22:44.989
Alexander Mayrhofer: as it does now, and really do like post registration.

570
01:22:45.803 --> 01:22:49.020
Alexander Mayrhofer: assessment, and then potentially verification.

571
01:22:50.530 --> 01:22:51.030
Alexander Mayrhofer: So.

572
01:22:51.030 --> 01:22:51.750
Polina Malaja: Picked.

573

01:22:51.750 --> 01:22:57.579
Alexander Mayrhofer: There is no application for domain name. It's just a registration that is used to be like last 25 years.

574
01:22:59.680 --> 01:23:19.369
Polina Malaja: Perfect, and then very quick, quick, very quick. Another question, because I know both Nick, it and Nick mentioned and be yeah. And that's the last question we take so the question from Olivia to Alex when submitting verification data, in which case it would make sense to send a result failed.

575
01:23:22.440 --> 01:23:27.210
Alexander Mayrhofer: It would make sense if the registrar

576
01:23:27.870 --> 01:23:34.409
Alexander Mayrhofer: identifies that this is like a fake registration in the 1st place, and wants to get rid of the domain name as quickly as possible, but

577
01:23:34.610 --> 01:23:46.779
Alexander Mayrhofer: we actually found out that it. It makes it everything very complicated. So we we probably only implement the Msa. Success, and we leave the wait verification for the

578
01:23:46.950 --> 01:23:52.480
Alexander Mayrhofer: pass of test that I described before, and the registrar can always delete the domain. In the 1st place.

579
01:23:55.530 --> 01:24:09.579
Polina Malaja: Thank you very much, and I think yes, we have to close the session. Unfortunately for the other questions that were not addressed to specific speakers. I would ask my distinguished panelists to take a look and respond if necessary, and if you feel

580
01:24:09.580 --> 01:24:28.090
Polina Malaja: I will also try to keep a track and see if I can respond to remaining questions from this session. Thank you once again for Alex, Timo

and Michael for giving your insight. And yeah, I apologize for running a bit over time, but I think it was important that we address the questions in the QA. Pods.

581
01:24:28.398 --> 01:24:34.869
Polina Malaja: So yeah. So I wish everyone a great continuation of the workshop and Heidi back to you. Thank you.

582
01:24:35.360 --> 01:24:35.920
Polina Malaja: I.

583
01:24:35.920 --> 01:24:36.729
Hadia Elminiawi: Thank you so much.

584
01:24:36.730 --> 01:24:37.080
Alexander Mayrhofer: Thank you.

585
01:24:37.080 --> 01:24:37.810
Hadia Elminiawi: So

586
01:24:38.430 --> 01:25:05.690
Hadia Elminiawi: thank you so much, Paulina, and and thank you to all panelists. So I I would remind you that we have 20 min allocated at the end of the workshop for Q. And a. So again, if you have more questions, you can put them in the Q&A pod, and you can resume the discussion. Now, I would like to move to Simon Fernande. And Simon, the floor is yours.

587
01:25:08.610 --> 01:25:09.889
Simon Fernandez: Okay, thanks a lot.

588
01:25:10.877 --> 01:25:31.639
Simon Fernandez: Ken, yeah, I tried starting the video. It seems to have like a small problem. So I have to go without the video. Sorry you won't be able to see my face. I hope you can see the screen. Well, so Hello, everyonees. I'm a postdoc researcher at university in France.

589
01:25:31.650 --> 01:25:46.889
Simon Fernandez: and I'll be presenting a paper that we published recently in the Passive and Active Measurements Conference this year called, Who Is Right, an analysis of who is an adapt consistency. So it was a joint work with colleagues from the team.

590
01:25:46.920 --> 01:26:05.809
Simon Fernandez: In this paper we studied who is up and data registration. So you are all aware of what registration information is. It's your job, but a quick reminder of why we, as researchers and security experts may need it.

591
01:26:05.830 --> 01:26:33.729
Simon Fernandez: When we are studying a block domain. When experts try to blacklist the domain. When you are trying to detect some behavior, we may need additional data about about a domain like who sold the domain? Who bought the domain? Did they buy multiple domains in bulk at the same time? If there are email addresses to contact when we do some notification campaigns, if we detect some strange behaviors or misconfigurations.

592
01:26:33.760 --> 01:26:43.690
Simon Fernandez: And so all of this information, called registration information can be gathered at the moment through 2 main protocols who is an adap.

593
01:26:43.690 --> 01:27:08.669
Simon Fernandez: So let's start with the oldest one who is. It's an old protocol almost as old as the Internet. It's insecure, it's unsigned, unencrypted, but it's widely spread. Almost all Tld's provide. Who is server? However, the main problem with who is its vague human readable format that is not clearly defined.

594
01:27:08.820 --> 01:27:13.380
Simon Fernandez: meaning parsing, who is, can be a real challenge from time to time.

595

01:27:13.980 --> 01:27:33.810
Simon Fernandez: This is an example, like an extract of the Who is entry of Google Com. We can see information that we, as researchers or security experts are interested in. For example, the creation date, the name servers the registrar abuse contact email. So that's for who is.

596
01:27:33.960 --> 01:27:41.449
Simon Fernandez: However, when I said that phase is hard to pass. It's also because the human readable format.

597
01:27:41.450 --> 01:28:06.390
Simon Fernandez: for example, does not define the language that should be used as a consequence. We sometimes observe things like this, this is the who is entry for the Epson com bo domain, and, as you can see, part of it is written in Spanish, meaning, if you don't know Spanish, you will have some trouble finding the actual information that you need for this domain. As a consequence, it's hard to do some systemic analysis of

598
01:28:06.390 --> 01:28:14.150
Simon Fernandez: domains, because we have to manually parse every entry or build complex systems to pass them in our step.

599
01:28:14.310 --> 01:28:40.370
Simon Fernandez: Another problem that we have with who is our dates because dates are the bane of all computer scientists, and sometimes in some entries, we observe things like this, and then it's a complete disaster when we try to parse it. And because many different registries and registrars use different conventions, and we may have some difficulties finding the actual value that are interesting for us.

600
01:28:40.780 --> 01:29:04.489
Simon Fernandez: As a consequence, in 2,015. A new protocol is designed registration data access protocol to access this data. It's using Http for transport Tls for security and authentication of the server. It uses Json data format, and the data types are relatively well defined. However, it's not used by all Tlds.

601

01:29:04.590 --> 01:29:19.259
Simon Fernandez: All generic Tlds, through their icon agreement must have an Ldap server, but many country code Tlds do not provide an Ldap server right now, at the time of speaking.

602
01:29:19.470 --> 01:29:36.670
Simon Fernandez: So this is an example of a small extract of the Ldap entry of the same Google Com domain. As you can see, the same data is present compared to the who is entry. However, the format is completely different. And in this example it's

603
01:29:36.670 --> 01:29:51.640
Simon Fernandez: easier to parse for machines because it's just Json data. However, it's harder to read for humans, because you will have to know what an object class name like what every entry means. So it's harder to parse.

604
01:29:51.640 --> 01:30:15.939
Simon Fernandez: Also, Ldap is not ideal. It's still not ideal, because we also have some parsing difficulties for Ldap. Rfcs either are unclear or not followed, and, for example, sometimes name servers are either listed as a full character text like ns.x.com.

605
01:30:15.940 --> 01:30:20.780
Simon Fernandez: or sometimes they are stored as an array of labels like this.

606
01:30:20.790 --> 01:30:47.069
Simon Fernandez: So then, we have to find which format is used for the field, also the main Airdrop, Rfc. Directory references, 17 other Rfcs. And so, as a consequence, most implementations sometimes somewhere may have some impressions, or it gets hard for registries and registrars to actually follow all of the Rfc. Specifications.

607
01:30:47.070 --> 01:30:53.989
Simon Fernandez: And as a consequence, it's hard for us as researchers to actually parse the data out of this Json entry.

608
01:30:54.710 --> 01:31:16.890
Simon Fernandez: Some terms are sometimes unclear in the Rfcs. And some objects can be actually quite tricky to handle like the V card arrays that are arrays of arrays of arrays, and so it can get pretty complex to use on a daily basis. And that's only hand-picked examples.

609
01:31:16.960 --> 01:31:41.090
Simon Fernandez: And now let's talk about how to get who is and airdap entries with their protocols. Let's start with the simple one, the airdap protocol. So if we try to gather information about example com, we 1st extract the tld com, we match it inside of an iana bootstrap file that lists all Tlds and associated airdap servers.

610
01:31:41.090 --> 01:32:01.449
Simon Fernandez: and this tells us to ask, for example, registry com through the Https protocol, we contact this server, we get a Json entry. We parse it. We may have some keys, some data, and inside of this entry there may be a referral saying that additional data can be found at this different server.

611
01:32:01.450 --> 01:32:18.750
Simon Fernandez: We can then follow this redirection. Ask, for example, the registrar net to get a new Json entry. Some data may be common between both entries and some keys, some values may only be present in one of the 2 entries.

612
01:32:19.366 --> 01:32:21.230
Simon Fernandez: So that's for. And

613
01:32:21.280 --> 01:32:40.160
Simon Fernandez: now let's talk about who is. It starts pretty much the same way we extract the Tld from the domain name, and we match it with an iana provided list, saying, for example, to contact registry.com on Port 43. So the who is protocol dedicated port.

614
01:32:40.200 --> 01:33:02.430

Simon Fernandez: However, the community found that many who is servers were not actually present inside of the iana provided list. As a consequence, most tools nowadays use a community-built list that is actually stored on Github right now, that has many more servers. So you have a higher chance of finding the server you are looking for.

615
01:33:02.520 --> 01:33:27.980
Simon Fernandez: Once you find the server that you need to contact you contact it through Port 43 with the who is protocol, and you get a free form, human, readable text for the domain. Inside of this entry you may find so data, keys values, and you may find a referral also, or however you spell a referral in Spanish, Korean, or Japanese.

616
01:33:27.980 --> 01:33:55.839
Simon Fernandez: So if you manage to actually find this referral somewhere in the entry. You may follow it and ask a new server through Port 43. Still, to get a new free form. Txt entry may be following a different format compared to the registry level format, and as for Ldap, some keys may be common between the registry entry and the registrar entry, and some keys may be specific to one of the

617
01:33:55.840 --> 01:34:24.119
Simon Fernandez: of the different entries. As a researcher, then we had the following question, there are multiple servers and records. For one example, com domain. Do they all provide the same that if I try to gather the registration date from Ldap, and who is does it matter if I ask through the other protocol, if I ask the registry or the registral servers. So that's the main question that we wanted to answer in this research work.

618
01:34:24.260 --> 01:34:36.080
Simon Fernandez: So to do this, we ran a huge survey. So we started from the list of domains aggregated from the Czeds Project, Passive Dns and public blacklists.

619
01:34:36.100 --> 01:34:55.600
Simon Fernandez: We selected 55 million domains that had both a who is and an adap server accessible, and we scanned them to collect all of their

records. So because each domain can have multiple records. As I presented before, we had 1, 64 million records for those 55 million domains.

620
01:34:55.600 --> 01:35:06.620
Simon Fernandez: we then passed those recalls with great difficulties as pointed before, and we checked if the values were actually consistent between who is Ldap and the different servers.

621
01:35:06.770 --> 01:35:30.610
Simon Fernandez: we selected those following fields to check the consistency of the data. So we selected those fields because they are used by other research work and are present in most records, because there are some fields that are present in a few percent of the records that are register specific that would like be difficult to compare.

622
01:35:30.610 --> 01:35:37.390
Simon Fernandez: So we selected name servers, creation and expiration date, Id and contact emails

623
01:35:37.580 --> 01:35:56.029
Simon Fernandez: in this presentation. So this is the generic results that we found. So in this table. For each field there is the missing rates, meaning it's the percentage of entries where either the entry was not present. The field was not present.

624
01:35:56.030 --> 01:36:17.449
Simon Fernandez: or we were not able to parse it or extract extract it in a meaningful way. So the missing rates fluctuates a little bit, and then we have the domain inconsistency meaning, it's the percentage of domains where at least 2 records for the same domain do not agree on this value.

625
01:36:17.450 --> 01:36:35.030
Simon Fernandez: So those values can be as low as 0 point 2%, for example, for the Id, and it climbs up to 4, 5% for other fields. The emails fields are a special case that we may talk about later. If we have time. During the questions

626
01:36:35.120 --> 01:36:46.630
Simon Fernandez: in this presentation, I'll focus on the name server case as an example of what we observed.

627
01:36:46.670 --> 01:37:15.029
Simon Fernandez: So for name servers, because each entry can provide multiple name servers, we have to compare lists, sets of name servers. As a consequence, we have different types of mismatches. 2 entries can disagree. For example, one entry may be included in the other entry. They can intersect having some name servers in common, but not all of them, or they can be completely disjoint.

628
01:37:15.070 --> 01:37:38.299
Simon Fernandez: We observed the following repetition of errors, so this is only considering the mismatches that we observed. So we observed that around 40% of cases we have an inclusion. So one entry who is held up included in the other entry, we have 4% of intersection and 60% of disjoint cases.

629
01:37:38.300 --> 01:37:50.680
Simon Fernandez: This does not sum up to 100%, because, as you remember, one domain can have 4, 5 6 entries, meaning you can have different types of mismatches for each domain.

630
01:37:50.950 --> 01:38:12.929
Simon Fernandez: In our work. We focused on the disjoint case because in our opinion, it is the most problematic one, because if in the inclusion or intersection case there are at least one name server in common meaning that maybe it just means that all the name servers actually provide the same data.

631
01:38:12.980 --> 01:38:33.080
Simon Fernandez: however, for the disjoint case, it means that there is no name servers at all in common between the 2 entries, meaning, it may mean that the different name servers listed in the who is, or lap entries do not provide the same data. So let's focus on this join case.

632
01:38:33.380 --> 01:38:57.399
Simon Fernandez: Remember this setup. We can have different type of mismatches. Mismatches can be between 2 entries of the same protocol. For example, the registry erdap entry, not agreeing with the registrar Ldap entry, or we can have mismatches between 2 different protocols. For example, the registry aired up entry, not agreeing with the registry who is entering.

633
01:38:57.650 --> 01:39:15.390
Simon Fernandez: we checked which one was the most common, and we observed that in 25% of the cases the mismatch was inside of one protocol, and in 75% of cases the mismatch was between 2 different protocols. So who is entry? Not agreeing with an Ldap entry

634
01:39:15.890 --> 01:39:35.300
Simon Fernandez: in the case of name servers, we are lucky because the Dns actually can provide ground truth. We have a 3rd party that provides us with the real value. We have big quotation marks of the Nsm. 3. So, as a consequence, we collected the Ns. Records from the Dns to check

635
01:39:35.300 --> 01:40:04.269
Simon Fernandez: when who is entered up disagree? Who has the right value? Who can we trust to get this specific name server value? And we observed that in 21% of the cases who had the right name server set in 78.5% of cases. Airdap had the right name server cases, and in the remaining point 5% of cases, neither who is Norap actually agree with the Dns values.

636
01:40:04.670 --> 01:40:26.889
Simon Fernandez: 78.5% of the cases is big. So we may think that. Okay, we can trust Ldap. However, we still have 20% of cases where Ldap has the wrong does not agree with the Dns at least, and the Dns approved values are actually stored in the horizontal.

637
01:40:27.020 --> 01:40:51.709
Simon Fernandez: and so for other. So this is the special case for for name servers, but for name servers. We are lucky because we have the Dns

ground truth for other fields. We have no way of knowing who has the actual value for creation and expiration date. We have no other way to get those values outside of who is an adapt

638
01:40:51.820 --> 01:41:20.769
Simon Fernandez: as like outsiders from the registry point of view. And then we have some mismatches. That may be okay. For example, if entries do not agree, but only at a 1 day difference? Is it a huge problem? And then some entries actually use the iana id as an internal usage field, even if they are not concerned with Iana. For example, some country code use the iana Id field for their internal purposes

639
01:41:20.770 --> 01:41:35.929
Simon Fernandez: and also emails provided some great challenges through the Gdpr and the proxy setups. So, as a consequence for researchers and security experts. It's hard to get trust in those values.

640
01:41:36.240 --> 01:41:53.050
Simon Fernandez: Let's conclude this presentation. So registration information is used by researchers and experts to classify domains to detect trends to detect behaviors in registration, to detect abuses, to notify domain owners.

641
01:41:53.050 --> 01:42:14.489
Simon Fernandez: But those pieces of information can be found at different places through different protocols at different levels different servers. And even if Ldap is in the right direction with the ease of parsing this data, it's not there yet. There are still challenges for for adap.

642
01:42:14.590 --> 01:42:39.180
Simon Fernandez: We collected 1, 64 million records from 55 million domains across all Tlds. And we observed that around 5% of them have at least 2 records not agreeing with each other. As a consequence, in most cases we have no clear source of truth compared to name servers where we had the Dns to tell us who has the right value.

643
01:42:39.380 --> 01:42:55.059

Simon Fernandez: And so as users for this kind of data, researchers and security experts, we should use this data with care, because we don't know if the values we got are actually the right one, and it's hard to find a ground truth.

644
01:42:55.606 --> 01:43:23.690
Simon Fernandez: So all the data sets. We collected the past, who is in other countries and the Dns records can be downloaded freely. They are all open access online. Also, the code used to analyze this data is in open access, and if you are looking for a full written description of this project, and more in-depth detail for the other fields. You can just check our paper published at Pam this year called, Who Is, Write an analysis of that consistency.

645
01:43:23.850 --> 01:43:28.649
Simon Fernandez: Thanks a lot for your attention. So if you have questions, I'll be happy to to answer them.

646
01:43:30.132 --> 01:43:48.199
Hadia Elminiawi: Thank you so much. Simon. This is Hadia again for the record. So we have a question in the QA pod from Patrick de he says, do you do only one extract per? Or maybe I can give the floor to Patrick. Patrick, are you able to speak?

647
01:43:57.940 --> 01:43:58.833
Hadia Elminiawi: Okay. So

648
01:43:59.280 --> 01:44:01.570
Steve Conte - ICANN Org: I just. I'm sorry I just enabled his mic.

649
01:44:01.600 --> 01:44:02.890
Steve Conte - ICANN Org: Patrick, are you there.

650
01:44:07.140 --> 01:44:13.480
Simon Fernandez: So I can. Yeah, I can read his his question on the on the Q. And a, if if needed.

651
01:44:14.230 --> 01:44:14.850
Simon Fernandez: up.

652
01:44:14.850 --> 01:44:17.469
Hadia Elminiawi: Okay, so go ahead. Yeah.

653
01:44:18.100 --> 01:44:27.970
Simon Fernandez: So the question is, if I only extract, if I only do, one extract per domain and protocol or multiple ones during multiple times.

654
01:44:28.000 --> 01:44:44.360
Simon Fernandez: because discrepancies can be temporary flukes due to changes. So this analysis was not an analysis all the time, so we did not rescan the whole 55 million domains.

655
01:44:44.450 --> 01:45:02.449
Simon Fernandez: however. So we considered this especially, for, for example, creation, date and expiration date we checked, if, like, how big was the difference between who is another app or the different entries, and we plotted the differences. And so

656
01:45:02.530 --> 01:45:08.340
Simon Fernandez: the person, the amount of mismatches that we detected. Hence, like

657
01:45:08.370 --> 01:45:16.859
Simon Fernandez: we, we think that the percentage of mismatches is quite high for it to be. Only temporary. Flux.

658
01:45:16.860 --> 01:45:38.539
Simon Fernandez: like 5% of domains, are not being like it can happen to just collect data at the who is level while it is getting propagated through Ldap. But to get 5% of domains in those cases, it's still a big, a bit higher, in our opinion, a bit too high, in our opinion, to completely account for this amount.

659
01:45:38.540 --> 01:46:02.830
Simon Fernandez: and also when we ran the name server Dns analysis, we reconnected all the who is in other countries for the domains that had name, server, mismatches, and we detected, like the vast majority of domains, still had the same name server mismatches 3, 4 months after the 1st collection.

660
01:46:02.830 --> 01:46:18.199
Simon Fernandez: so we did not do a full recollection of the data a few months after. But for what we observed, it looks like. There may be some temporary flux in the data set, but we do not think that it is representative of the majority of domains.

661
01:46:20.040 --> 01:46:32.240
Hadia Elminiawi: Thank you so much, Patrick, for this answer, and we have a hand from Edward, and then I will read another Q. And a. Another question from the Q. And a pod. Edward. Please go ahead.

662
01:46:32.730 --> 01:46:46.030
Edward Lewis: Okay? So regarding no ground truth what I would suggest is, if you could take these mismatches and find out which registry maybe the largest. What has the largest number of mismatches or the largest registries.

663
01:46:46.070 --> 01:46:57.399
Edward Lewis: and try to contact them, explaining what your research is, and either find out if they can explain why there's a difference between these 2, they should be coming from the same ground. Truth, the same database, either.

664
01:46:57.400 --> 01:46:58.170
Simon Fernandez: Yeah.

665
01:46:58.170 --> 01:47:03.830
Edward Lewis: Aware of why, or maybe they're unaware of it. I would suggest a follow up to to actually talk to the registrar.

666
01:47:04.510 --> 01:47:16.560
Simon Fernandez: Yeah, we did this for the Ayana id example, the specific case of Ian Ids, where it was clear that, for example, there were some invalid Ayana ids in some entries.

667
01:47:16.560 --> 01:47:39.779
Simon Fernandez: So entries, mismatching, and with one of the values being completely invalid Id. And so in those cases we contacted the registry and registrars to tell them that there is a mismatch somewhere. We registered our own domains with their services to check. If it was a 1-time problem or a systemic problem. And we found that it was a systemic problem because

668
01:47:39.780 --> 01:47:47.250
Simon Fernandez: newly registered domain had the same problem. So we contacted them. We tried to get some additional information on their part.

669
01:47:47.250 --> 01:48:17.180
Simon Fernandez: and we had no feedback from their part. But a few months later, when we ran our scan for those specific domains, all those mismatches for the registrars that we contacted disappeared. So in this specific case we observed that the iron Id was wrong. There were some placeholder emails and phone numbers. So it looked like default placeholders, values that were not modified the right way.

670
01:48:17.290 --> 01:48:46.499
Simon Fernandez: I don't know if it was following our questions to them, but at least in the months that followed they fixed their systems and all the domains got updated. But yeah, the main difficulty is to actually know who to contact, and because, like registries like, it's pretty rare to have one registry that has a hundred percent mismatch in one field sometime is just like, strangely, 5% of their domain have a mismatching creation date.

671
01:48:46.600 --> 01:49:10.549
Simon Fernandez: And so yeah, as a follow-up research topic for us, yeah, we would like to to do a more widespread notification campaign to registration registrars to check with them where this may come from,

because, as external measurements, we have no way of knowing. Where do they come from? Where those mismatches come from?

672
01:49:11.550 --> 01:49:20.350
Edward Lewis: Yeah. So so I'd like to follow up with that, I think it's yeah. It would also be interesting in your. So I don't like to name and shame. I don't like you to to name who is the most out of whack.

673
01:49:20.470 --> 01:49:26.019
Edward Lewis: but I think it's good to categorize it. So we know so the community gets to know which how to kind of attack

674
01:49:26.110 --> 01:49:37.115
Edward Lewis: of this issue, whether it's individual contacts to smaller registries or it's a larger registry. That's the source of this that I I like to know the shape of what needs to be done, but not to answer for now, but I would suggest that.

675
01:49:37.360 --> 01:50:04.260
Simon Fernandez: There is if you want. So in the paper we plotted in the Annex a map of amount of percentage of mismatching domains compared to the size of the Tld to check if there are some tendencies, and so we have pretty much everything. We have some big Tlds that have a high mismat rate. We have some small Tlds that have a low mismatch, but also, like we have it in all the possible directions.

676
01:50:04.260 --> 01:50:20.189
Simon Fernandez: So one thing that we may do is to contact the Tlds and registries and registrars that have the highest mismatch amount, because it may mean that there is a systemic problem on their side compared to just some small problems. So, yeah.

677
01:50:20.250 --> 01:50:22.499
Simon Fernandez: so a great idea. Thanks.

678
01:50:24.500 --> 01:50:43.009

Hadia Elminiawi: Thank you, Simon. Could I? Just go in with a question here. So you said you follow going forward? You would contact registries registrars. So in order to know more. And I was wondering, do do you contact both, or is it enough to contact the registries? And they contact the registrars.

679
01:50:43.900 --> 01:51:08.739
Simon Fernandez: The way we did it is we contacted the registrars because it was easier to like some some registries that we tried to contact some registrars, sorry that we tried to contact, just told us that they will not answer us if we are not their customers, so we had to limit our contact points to the registrars where we were

680
01:51:08.740 --> 01:51:26.550
Simon Fernandez: able to like, buy a domain and ask the question as customers compared to researchers that are highlighting a problem. But yeah, a more in-depth analysis, where we could directly contact the registries is a great idea. Yeah.

681
01:51:27.230 --> 01:51:48.879
Simon Fernandez: And in any case, if you want to take a look at the the data that we extracted, all the data set and code is public. So if you are worried that your registry or registrar is having some problems on this part feel free to just get the data sets, and all the data is freely accessible through this.

682
01:51:50.010 --> 01:52:02.960
Hadia Elminiawi: Thank you so much, Simon, and there is a question in the Q. And a pod from Olivier. He says, in regards to data mismatch. Do you take into account that most who is servers delay, information.

683
01:52:03.870 --> 01:52:20.469
Simon Fernandez: Yeah. So it was one of our main worries that like data is probably updated at one central server and then slowly updated through who is on the other app and the different servers through different protocols.

684
01:52:20.470 --> 01:52:45.460

Simon Fernandez: And so this is what I answered in the beginning, meaning that it could amount for a few specific case where, okay, bad luck. We collected the creation date right when the domain was being transferred boards or etc. But the amount of mismatches that we observed made us think that it is not

685
01:52:45.460 --> 01:52:48.190
Simon Fernandez: not the only source of problems.

686
01:52:48.190 --> 01:53:14.080
Simon Fernandez: and the fact that also, when we contacted some registrars on those specific problems. There were some actual problems on their side. It was not only a propagation problem, but it's 1 difficulty of this analysis is that we should do some long-term analysis, but then handle both cases where the domain actually changed, or where the data was just being propagated through the infrared servers.

687
01:53:14.080 --> 01:53:20.800
Simon Fernandez: So we chose to do it. The simple way for this for this beginning paper.

688
01:53:22.526 --> 01:53:39.970
Hadia Elminiawi: Thank you so much. Simon. And then you have a comment in the Q. And a pod from Roger. He says, just a comment, I think assuming Dns is right, could be a prospective issue. This is how things are functioning technically, but it may not be what the domain owner, slash registrant, would consider right.

689
01:53:40.280 --> 01:54:05.979
Simon Fernandez: Yes, that's absolutely true. The way we described it was that the main usage for the name server entries in the adap entries are like. There are not a lot of researchers and security experts that use this name server entry directly, because most of researchers.

690
01:54:05.980 --> 01:54:33.880
Simon Fernandez: if they want the name servers, they actually ask the Dns instead. So yeah, it's not the right value, as Roger described. It's just that if

the goal of the name server entry is to describe which name server is authoritative. For this domain, then Dns has a bigger weight on this matter compared to who is, or Ldap that are not part of any domain. Resolution, for example.

691
01:54:36.220 --> 01:54:39.840
Hadia Elminiawi: Thank you, Simon. Again, and with.

692
01:54:39.840 --> 01:54:40.250
Simon Fernandez: Thanks.

693
01:54:40.656 --> 01:55:03.023
Hadia Elminiawi: That I would like to. Thank you, and we have a 10 min break now instead of 15, please. Don't be late. Come back on time, and we can resume our discussions. We have an open discussion item at the end of the workshop.

694
01:55:04.120 --> 01:55:05.730
Hadia Elminiawi: So we start the break

695
02:05:41.670 --> 02:05:43.950
Hadia Elminiawi: so welcome. All

696
02:05:47.840 --> 02:05:58.329
Hadia Elminiawi: this is Hadia again for the record. I hope you had a good short break, and are feeling refreshed and ready to continue with a workshop.

697
02:05:58.785 --> 02:06:06.629
Hadia Elminiawi: Now we move to Gavin Brown from icam Gavin, the floor is yours.

698
02:06:06.920 --> 02:06:11.729
Gavin Brown - ICANN Org: Thank you. Heia! Hi, everyone. So to pick up for my

699
02:06:12.170 --> 02:06:15.100
Gavin Brown - ICANN Org: presentation today is what I'm calling stealth, rat

700
02:06:15.781 --> 02:06:21.010
Gavin Brown - ICANN Org: and if we can move on to next slide. I'll just briefly outline what I'm going to be talking about.

701
02:06:24.760 --> 02:06:26.210
Gavin Brown - ICANN Org: and we have the next slide.

702
02:06:27.000 --> 02:06:49.840
Gavin Brown - ICANN Org: There we go. So just briefly discussing background to this issue. About how that service discovery works. How are that clients? Implement service discovery what the deployment timeline timeline for audap looks like in the different types of registries that that is designed to to be implemented by describing what stuff are that looks like

703
02:06:50.225 --> 02:06:57.529
Gavin Brown - ICANN Org: how I found some stealth adapters, and what the impact of stealth adapt is on the overall ecosystem and community.

704
02:06:58.125 --> 02:07:02.610
Gavin Brown - ICANN Org: So next slide, please. So just just to kick off the discussions.

705
02:07:02.660 --> 02:07:27.589
Gavin Brown - ICANN Org: just posing an age. Old philosophical question for you. If if the tree were to fall in an island where there were no human beings, would there be any sound? This is something that I think most of us know in one form or another. This is the original source of that of that of that question. So keep that in mind when you're thinking about what I'm talking about now. So let's move on briefly to discuss the on the next slide topic about that service discovery.

706

02:07:28.120 --> 02:07:56.430
Gavin Brown - ICANN Org: So, as you will know. And in fact, it was discussed on the previous presentation. Who is never had any way to find out which. Who is server, was the right? Who is server for a particular query. The only way to really find out was to kind of develop, maintain various ad hoc ways of doing it. So now Iana never really had a a record of every single server. People had. You know, their own libraries and dictionaries that they used

707
02:07:56.925 --> 02:08:16.589
Gavin Brown - ICANN Org: and service discovery was not originally something that the that that that was a deliverable for the working group which produced our debt. But they did eventually produce the Rfc. 7, 4, 8, 4 which defines a bootstrap registries for the different types of objects that Rdp supports.

708
02:08:16.730 --> 02:08:18.300
Gavin Brown - ICANN Org: Next slide, please.

709
02:08:18.790 --> 02:08:29.640
Gavin Brown - ICANN Org: So let's see how many Rdap clients actually use those iana registries, and the answer to that question is pretty much all of them. So a few of these are

710
02:08:30.065 --> 02:08:33.915
Gavin Brown - ICANN Org: pieces of code that I maintain in my own capacity.

711
02:08:34.320 --> 02:08:58.570
Gavin Brown - ICANN Org: some of them are published as commercial products. Some of them are open source. Some of them are libraries, some of them are actual clients. You can see pretty much all of them, in fact, all of them. Use the iana registries so you can give them a domain name or an IP address and it will know how to find the that server for that resource. If one is present in the Bootstrap registry.

712
02:09:00.120 --> 02:09:15.319

Gavin Brown - ICANN Org: So what can we conclude from that? On the next slide we can look a little bit about what the conclusions for that is the firstly if you're using an off the shelf client, whether it's open source or otherwise. They all support bootstrapping, using a registry

713
02:09:15.320 --> 02:09:30.240
Gavin Brown - ICANN Org: and a corollary of that. So the a kind of subsequent conclusion is that if a a Tld doesn't have an entry in that bootstrapped file, it's essentially invisible to users of those clients

714
02:09:30.250 --> 02:09:36.930
Gavin Brown - ICANN Org: unless they manually manually specify it, and not all clients provide for that facility.

715
02:09:39.030 --> 02:09:40.140
Gavin Brown - ICANN Org: next slide.

716
02:09:40.840 --> 02:09:59.190
Gavin Brown - ICANN Org: So let's go back to our question about a tree falling in the woods and rephrase it in the context of our Dep. So if someone at a registry deploys our our depth service, but doesn't tell anyone about it. Did they really actually deploy an art app service? Because if you can't reach it, then it doesn't really matter whether it's there or not.

717
02:10:01.380 --> 02:10:24.329
Gavin Brown - ICANN Org: So let's move on to the next section of this discussion, which is just to talk briefly about the ilap deployment timeline. So on the next slide. We talk about how it looks in the the regional Internet registry space, or the number space. Pretty much every single IP address with Ipv. 4 or Ipv. 6, or as number has an addressable Id record.

718
02:10:24.715 --> 02:10:44.350
Gavin Brown - ICANN Org: And this works partly because the the bridge truck registries are, you know that cover all of the allocated space in those names number spaces, but also because of cooperation between rais to put redirections in place, but that what that means is, if you're cons trying to consume data

719
02:10:44.560 --> 02:10:49.509
Gavin Brown - ICANN Org: about numbers using Rdap, you can rely on

720
02:10:49.820 --> 02:10:50.830
Gavin Brown - ICANN Org: those

721
02:10:51.327 --> 02:10:54.460
Gavin Brown - ICANN Org: those resources to have an Rdp record.

722
02:10:55.703 --> 02:10:59.339
Gavin Brown - ICANN Org: Let's look at the Gtd. Space on the next slide.

723
02:10:59.850 --> 02:11:06.599
Gavin Brown - ICANN Org: So since 2,019, Idep is mandatory for all Dt registries and registrars

724
02:11:07.107 --> 02:11:18.922
Gavin Brown - ICANN Org: and all Gt domains have an audit record accessible in in principle, because every single Gt has an entry in the Bootstrap registry. So again, if you're looking to

725
02:11:19.936 --> 02:11:32.153
Gavin Brown - ICANN Org: consume registration data about gts, in principle, you should be able to rely on being able to use adap to do that. Obviously, there are some

726
02:11:33.630 --> 02:11:50.549
Gavin Brown - ICANN Org: situations where that's not going to be true service. Go down. Server responses, as we've seen again in the previous response are not always as reliable as we like. They don't always have the data that they need to have, but in principle it should be possible to get an audit record for every single Gtm that exists.

727

02:11:51.400 --> 02:11:53.999
Gavin Brown - ICANN Org: How does this compare to the CCTV world?

728
02:11:54.920 --> 02:11:57.808
Gavin Brown - ICANN Org: On the next slide? We can look so

729
02:11:58.530 --> 02:12:02.449
Gavin Brown - ICANN Org: obviously deployment there is is, is somewhat slower.

730
02:12:03.170 --> 02:12:16.079
Gavin Brown - ICANN Org: that's despite the fact that actually the 1st Cctlds or the 1st Tld's to be added to the inner registry were, in fact, Ccts. But with with the 1st Gtlds only coming sub some some months later.

731
02:12:16.423 --> 02:12:33.589
Gavin Brown - ICANN Org: But as things currently stand, only 14% of all Cctvs have an audit server at the moment. And only about 25% of domains under management in those Cctvs have an accessible audit record. So if you're looking at designing something that's going to consume registration data.

732
02:12:33.993 --> 02:12:44.630
Gavin Brown - ICANN Org: That needs to account for Ccts. It's a reasonable question to ask as to whether it's worth putting the effort into supporting our data for those Cctlds.

733
02:12:47.010 --> 02:13:15.420
Gavin Brown - ICANN Org: So let's move on to the next section of topic, which is the main me to this presentation, which is the topic of stealth. Rd, so let's go on to the next slide. So so I run Rdto org in my personal capacity as a as a Bootstrap server where people can. If they're writing a 1 off script, just construct a URL using rd.org, and it will get redirected to the right place, and the most common support question I get from people sending me email is, why doesn't rdap support

734

02:13:15.460 --> 02:13:33.100
Gavin Brown - ICANN Org: so and so, whether that's a CCTV or or something else, and when I look, what happens is almost always the case that the registry cctld registry has has turned on our depth, turned on our depth server on, but hasn't told anyone about it. It's not in the Bootstrap registry.

735
02:13:33.478 --> 02:13:38.249
Gavin Brown - ICANN Org: Which is where I come to the conclusion that to call this stealth R. Dep.

736
02:13:38.280 --> 02:13:47.660
Gavin Brown - ICANN Org: Because, just like a stealth name server, a stealth. So Rd server exists. But there's no way for anyone on the Internet to find out about it.

737
02:13:47.770 --> 02:13:53.529
Gavin Brown - ICANN Org: at least in band, as part of the bootstrapping mechanism that adap has built into it.

738
02:13:53.832 --> 02:13:58.349
Gavin Brown - ICANN Org: I made a decision early on that, on that org would only ever use the vanilla

739
02:13:58.390 --> 02:14:19.849
Gavin Brown - ICANN Org: Bootstrap registry from my Anna Anna, so it doesn't have any hard coded entries for for these adap servers, and I think you'll find that probably most of those are that clients that I mentioned on the previous slides do the same thing. We don't want to be maintaining our own sets of of exceptions to the Bootstrap registry, because that's what the Bootstrap registry is for

740
02:14:20.850 --> 02:14:21.700
Gavin Brown - ICANN Org: sight.

741
02:14:22.360 --> 02:14:30.159

Gavin Brown - ICANN Org: I decided to carry out a survey, and on on the next slide. I talk about trying to find out how many stealth rip servers there actually are.

742
02:14:30.250 --> 02:14:39.669
Gavin Brown - ICANN Org: So this is something I did sort of. I've done several times over the last few months. 1st time I did. It was earlier late last year.

743
02:14:40.046 --> 02:14:51.759
Gavin Brown - ICANN Org: But the the results I'm gonna present today are from last week. So what I did was extract domain names and host names that appear in who is records

744
02:14:51.790 --> 02:15:00.149
Gavin Brown - ICANN Org: in the inert tld database for all the Cctl. Ds that don't already have an entry in the Bootstep registry.

745
02:15:00.340 --> 02:15:01.900
Gavin Brown - ICANN Org: and then for

746
02:15:02.460 --> 02:15:15.149
Gavin Brown - ICANN Org: each one of those domain and host names, I generate a list of potential are that post names based on domain names appearing in the email addresses their website domain, who is server

747
02:15:15.886 --> 02:15:38.429
Gavin Brown - ICANN Org: and then construct a set of Urls based on those host names. Using kind of common patterns that you can see if you look at the Bootstrap registry. You know how how bootstrap base urls are are prefixed with certain common patterns like slash v 1, or slash tld or slash Rd app and then try and can perform a help. Query

748
02:15:39.093 --> 02:15:46.670
Gavin Brown - ICANN Org: and then depending on the results. It sort of flag whether or not what I see looks like. It might be an Rd app server.

749
02:15:47.090 --> 02:15:55.059
Gavin Brown - ICANN Org: So just getting a Json response back with a 200 status is is enough to indicate. This is probably an art app server and not something else.

750
02:15:55.730 --> 02:15:59.950
Gavin Brown - ICANN Org: So what did I find on the next result? On next slide are the results.

751
02:16:00.100 --> 02:16:07.471
Gavin Brown - ICANN Org: So I was able to find 13 stealth art app servers. The previous runs I found more.

752
02:16:07.920 --> 02:16:28.999
Gavin Brown - ICANN Org: but what's actually happened is that those servers have ended up going into the Bootstrap registry. And that's obviously good news, because that means that there's more accessible. Rdp, in the world. But it it goes to show this is kind of a moving target. So I found 13 stealth Rd service, and you can see some of the cctodes here are not insignificant Cct. And

753
02:16:29.000 --> 02:16:42.089
Gavin Brown - ICANN Org: Highlight. Some of the most notable ones. That collectively represent 25% of all domain names registered under Ccts. So from a user's point of view, that's a big chunk of the namespace which is

754
02:16:42.200 --> 02:16:56.630
Gavin Brown - ICANN Org: invisible, which need not be invisible. If they were added to the Bootstrap file, then that percentage of CCTV domains that would be accessible via our data would double. It would go from about 25% to about 50%

755
02:16:56.955 --> 02:17:24.209
Gavin Brown - ICANN Org: and the overall level of coverage for all domain names under management in the entire namespace would increase to 82%.

So again, if you're thinking about how you want to access registration data, whether you do it using old school Port 43, or whether you want to do it using our app. It changes the the the kind of decision you might want to make about. You know what's protocols you're going to support. Should I go to the effort of supporting our app? Or should I rely on? Who is because it's more accessible?

756
02:17:24.879 --> 02:17:29.359
Gavin Brown - ICANN Org: So, having found all these Upstaff art app service, I wanted to ask myself.

757
02:17:29.660 --> 02:17:37.530
Gavin Brown - ICANN Org: why why would this be. Why would this not happen? And some of these startup service, I know, have been around for some time.

758
02:17:38.273 --> 02:17:40.329
Gavin Brown - ICANN Org: So this next slide

759
02:17:40.389 --> 02:17:42.659
Gavin Brown - ICANN Org: really is me kind of

760
02:17:43.155 --> 02:17:57.499
Gavin Brown - ICANN Org: putting myself in the position of a CCTV operator which I have been in the past and trying to understand. You know what the problems that they might be facing. Because obviously, if we can think about what these problems are, then they might be that we, as a community, can help

761
02:17:57.911 --> 02:18:25.340
Gavin Brown - ICANN Org: solve them. So the 1st reason would be, obviously, if you're in the process of deploying our dev, then you're not ready to to to add your till your your base URL to the Bootstrap registry yet, because you're still building infrastructure, you're still testing. You're not ready for production mode and maybe there are stakeholders in your community that you you want to prioritize communication with first, st

before you open the floodgates and allow the whole world to access. Your adap service

762
02:18:25.830 --> 02:18:31.759
Gavin Brown - ICANN Org: that is completely reasonable and is, is understandable.

763
02:18:32.260 --> 02:18:39.200
Gavin Brown - ICANN Org: Obviously there are those who simply didn't know that it was a core part of the yard app

764
02:18:39.389 --> 02:18:57.900
Gavin Brown - ICANN Org: protocol is the Bootstrap registry, which again is, is is not unreasonable. No one's under any obligation to implement every single Rfc and so. Perhaps this is something that you know. They feel that they've done enough by implementing the service. And and they're just that's enough for them.

765
02:18:58.564 --> 02:19:17.089
Gavin Brown - ICANN Org: It might also be that the the the idea of exposing the art of service and making it accessible to the whole world just isn't aligned with their goals as an organization. They care about their local community. And they have good relationships with those people. They can send them an email. They can knock on their door. They can

766
02:19:17.180 --> 02:19:28.390
Gavin Brown - ICANN Org: whatever talk about their adapter service in private meetings, so they can find out the yard server for that CCTV. Out of band, and therefore there's no need to add it to the Bootstrap registry.

767
02:19:28.540 --> 02:19:46.530
Gavin Brown - ICANN Org: And then there's the other one at the end. Which again, I've been here, and I've seen this as well is because it requires a a route zone. change or route zone management system change to add a a base URL to a to a record in the I know who is database or registry database.

768
02:19:46.830 --> 02:19:59.230
Gavin Brown - ICANN Org: that requires approval, and it goes up to to the, to the administrative contact. And that involves having conversations that can sometimes drag out and become

769
02:19:59.230 --> 02:20:03.460
Gavin Brown - ICANN Org: more complicated than it's necessarily worth pursuing.

770
02:20:04.340 --> 02:20:25.250
Gavin Brown - ICANN Org: There may be other reasons why. The cctld might choose not to register their base URL with the Anna and I guess one of the things I'm I'd be kind of quite keen to hear is from other people who are on this session, who are at a cctld that hasn't yet why, that might be, because again, what we want to do is try and find

771
02:20:25.350 --> 02:20:27.120
Gavin Brown - ICANN Org: solutions to these problems.

772
02:20:28.530 --> 02:20:31.900
Gavin Brown - ICANN Org: So why does this matter? Let's look at the next slide.

773
02:20:32.270 --> 02:20:36.909
Gavin Brown - ICANN Org: As I said before, because the way that all the the ide clients work

774
02:20:37.270 --> 02:20:42.439
Gavin Brown - ICANN Org: to use the Bootstrap registry if you deploy that. But don't add your

775
02:20:42.750 --> 02:20:50.139
Gavin Brown - ICANN Org: register. Your entry to the, to, the, to the registry. You're adding friction to the users, even those who you may have a close relationship to

776
02:20:50.610 --> 02:21:07.439
Gavin Brown - ICANN Org: who are within your community because they're still going to be using the the tooling that that everyone else is using, that they're getting off the shelf from Github or part of their operating system, or wherever, and you're making it harder for them to use the service that you've put a lot of time and effort into

777
02:21:08.670 --> 02:21:10.170
Gavin Brown - ICANN Org: into developing

778
02:21:10.591 --> 02:21:13.970
Gavin Brown - ICANN Org: and there's a lot of legacy code that depends on who is.

779
02:21:13.980 --> 02:21:18.500
Gavin Brown - ICANN Org: And that's never going to go away

780
02:21:18.850 --> 02:21:20.100
Gavin Brown - ICANN Org: until

781
02:21:20.110 --> 02:21:27.479
Gavin Brown - ICANN Org: the cost benefit analysis on the part of the of the people operating these these legacy systems

782
02:21:27.970 --> 02:21:32.370
Gavin Brown - ICANN Org: sort of moves into the right direction, because if they, if they

783
02:21:33.600 --> 02:21:40.370
Gavin Brown - ICANN Org: still if they can implement. That, but still have to support. Who is? That's a little huge pain they might as well just stick with who is

784

02:21:41.090 --> 02:21:41.710
Gavin Brown - ICANN Org: and

785
02:21:41.760 --> 02:21:58.615
Gavin Brown - ICANN Org: we need to kind of recognize that the Rf. Is better than who isn't the better for better for registries, better for registrants, better for the end users. And so everyone who who is on the who is on the Internet is is having a worse time of it.

786
02:21:59.010 --> 02:22:02.949
Gavin Brown - ICANN Org: all the time that Port 43 is around, and so we need to get rid of it.

787
02:22:03.740 --> 02:22:04.630
Gavin Brown - ICANN Org: So

788
02:22:04.960 --> 02:22:07.670
Gavin Brown - ICANN Org: last slide is really just to

789
02:22:07.880 --> 02:22:10.749
Gavin Brown - ICANN Org: just give some a gentle nudge

790
02:22:10.830 --> 02:22:11.670
Gavin Brown - ICANN Org: to

791
02:22:12.520 --> 02:22:25.989
Gavin Brown - ICANN Org: People at Cctld who have an Rdp. Server have a stealth, R. Dep. Server. It's very straightforward to add your base URL to the Boost registry. You go to the Iana route zone management system. Login

792
02:22:26.000 --> 02:22:46.949
Gavin Brown - ICANN Org: paste the URL into a text box. Hit, submit button. Someone has to go and approve that. But once it's done. It's usually fairly quick, then that that registry serve a base. Yeah. URL will appear appear in

the Bootstrap registry fairly quickly, and then it shows up on deployment to i.org, which is the system I run that keeps track of all this stuff.

793
02:22:48.190 --> 02:22:49.110
Gavin Brown - ICANN Org: So

794
02:22:50.170 --> 02:22:56.830
Gavin Brown - ICANN Org: yeah, so there we are. So so on the next slide. Just if anyone has any questions or comments, I'm looking forward to hearing that.

795
02:22:58.540 --> 02:23:13.091
Hadia Elminiawi: Thank you. Gavin, this is Hadi again for the record. And we have actually a comment and a question in the Q&A pod we also have a hand from Edward. Would you like to

796
02:23:13.460 --> 02:23:15.389
Hadia Elminiawi: to to read the Q&A.

797
02:23:16.310 --> 02:23:17.370
Gavin Brown - ICANN Org: Happy to. Yes.

798
02:23:18.740 --> 02:23:24.819
Gavin Brown - ICANN Org: So mark apologet points out that his audit Browser is not written in

799
02:23:25.617 --> 02:23:31.300
Gavin Brown - ICANN Org: Justin Swift. It's also in Kotlin. So that's noted. I will make sure that my slides get updated for the next time around.

800
02:23:33.080 --> 02:23:41.010
Gavin Brown - ICANN Org: So Mark also says what you define as stealth are. That is not just, not observer in some phases of testing pre-production, or not ready for scaling

801
02:23:41.090 --> 02:23:46.350
Gavin Brown - ICANN Org: before being published and giving a CCTV. No incentive to contractual deadline to be faster.

802
02:23:46.700 --> 02:24:04.355
Gavin Brown - ICANN Org: That's true. Yes. So so I'm looking for something that's accessible on the Internet. Whether that's ready for production or not I, I can't say. But it's on the Internet, so that, you know, there's some in certain implication that that that it's at least ready for someone to be having a look at, even if

803
02:24:04.670 --> 02:24:06.789
Gavin Brown - ICANN Org: it's not in the Bootstrap registry.

804
02:24:07.326 --> 02:24:18.590
Gavin Brown - ICANN Org: Given that many are actually operated by registrys that for the Gt's. Who already have implemented Rj. They may just offer the Cctvs version for the Ccds. They manage, but since they obligated, they just not publish it.

805
02:24:18.640 --> 02:24:21.000
Gavin Brown - ICANN Org: Maybe this is just a CCTV

806
02:24:21.240 --> 02:24:47.319
Gavin Brown - ICANN Org: Gtd policy issue. This is also true. Many Cccs make use of the same registry service providers that Gts do. You often get it essentially for free but the but would go back to that, that last option on the on the slide about. Why, this might not happen is, is that an rsp may be keen to to an offer our depth on

807
02:24:47.667 --> 02:25:05.979
Gavin Brown - ICANN Org: a CCTV. They run but having that conversation with the CCTV. Manager who may not necessarily be very accessible or reachable, may be interested in getting a you know, a a a monthly check, and that's about all they wanna hear back here from their rsp, just means it's not worth the effort.

808
02:25:08.260 --> 02:25:10.810
Gavin Brown - ICANN Org: shall we, Ed? Do you want to.

809
02:25:11.265 --> 02:25:11.720
Hadia Elminiawi: Edward.

810
02:25:11.720 --> 02:25:12.744
Gavin Brown - ICANN Org: Yeah.

811
02:25:14.060 --> 02:25:15.640
Gavin Brown - ICANN Org: yeah. And then get to Patrick. Yeah.

812
02:25:16.430 --> 02:25:22.169
Edward Lewis: Alright so Gavin, what like will you mind saying, Hello!

813
02:25:22.180 --> 02:25:34.479
Edward Lewis: Okay. The point, the thing I wanted to comment was, you said that. Oh, some of these, some the reasons for these cell servers. I'm sorry I had 2 things in my head cell service. I had be back 2 jobs ago

814
02:25:36.750 --> 02:25:50.490
Edward Lewis: I noticed that 2 2 particular Id and Ccts were all signed, but had no Ds record same similar situation right? At the time I was able to go up and ask the person like, what's going on there. And yeah, I was told, stood out.

815
02:25:50.750 --> 02:25:59.880
Edward Lewis: The administrator of that pair of Idns also had a cctld on the side. Didn't treat the Idns as Seri plds.

816
02:26:00.200 --> 02:26:21.513
Edward Lewis: he said. They're experimental. I don't really wanna make them fully secure. And so for for your work here. We're just thinking in some

of these cases where you see stealth ones out there, whether or not they are. 1st of all, they're persistent. Oh, by the way, I should add to that through my next job. They never did for the Ds record, and they're still in the same state after like over a decade

817
02:26:21.940 --> 02:26:38.380
Edward Lewis: and so and and we did put general pressure on them through other people to to see what they're going on. But the thing here is, I think it'd be good to measure this over time to see if they stay south or not, because you may. Some of the operators may have different ideas of why they've gotten into this. And I just wanna, I'll drop you on this

818
02:26:39.080 --> 02:26:40.740
Edward Lewis: hopefully. Thank you. Again.

819
02:26:42.420 --> 02:26:44.079
Edward Lewis: You said a hundred percent of old.

820
02:26:46.050 --> 02:26:47.189
Edward Lewis: Wonder if I covered

821
02:26:47.300 --> 02:26:48.290
Edward Lewis: the old.

822
02:26:49.680 --> 02:26:53.561
Hadia Elminiawi: Edward? Your audio is not clear. Could could you like

823
02:26:54.230 --> 02:26:57.366
Hadia Elminiawi: How closer to the mic, or raise your voice.

824
02:26:57.680 --> 02:27:15.680
Edward Lewis: Okay? I'd say, I know some of the class. A space is kind of wonky with some of the management of of the IP ranges, and I'm curious if that if you checked all of the class a space I mean the Irs may be fine. I

mean they they do everything. But there are a few other oddballs in there. So that's why I'm concerned about the 100% coverage number.

825
02:27:16.849 --> 02:27:33.479
Gavin Brown - ICANN Org: I I will be. I've not. I've not fully checked all of that. But, as as I say, the the Rs. Obviously do, they cooperate and do redirect to things. But there are some, some very so legacy allocations which may not be fully covered. That's that's that's true. Yeah. Yeah.

826
02:27:36.720 --> 02:27:44.840
Gavin Brown - ICANN Org: so yeah, now you're you're right about the your comment about kind of repeating this exercise. That is, that is my intention.

827
02:27:45.278 --> 02:27:57.401
Gavin Brown - ICANN Org: Some of the tld's that I found in the in the most recent survey. They have been in that situation for getting on for a year, if not longer. So

828
02:27:58.045 --> 02:28:26.489
Gavin Brown - ICANN Org: doesn't seem to be very volatile. But I will like, I said. Some of them, you know, proceeded to the to to to add their Urls to the Bootstrap registry, and and and that kind of you know, out the other end of that that deployment lifecycle. But but some of them are are stuck and really would be very interested in seeing, you know, talking to them and finding out why. But but you know, I would expect this change this list just kind of change periodically. So maybe I'll I'll do that on a quarterly basis and and keep track of that.

829
02:28:26.570 --> 02:28:28.310
Gavin Brown - ICANN Org: Yeah, thank you?

830
02:28:29.880 --> 02:28:39.329
Gavin Brown - ICANN Org: And then we have a comment from Patrick for discovery. Each registry, in fact, any source should be able to rely on serve records.

831

02:28:39.460 --> 02:28:44.089
Gavin Brown - ICANN Org: publish a fact that they have an art app server available compliance relying on that

832
02:28:44.913 --> 02:28:55.849
Gavin Brown - ICANN Org: it is used by at least one registry, for who is that would allow any public suffix to have a properly advertised on that app server. I don't remember. This is discussed in the itf with rejects working group, so

833
02:28:56.070 --> 02:28:59.889
Gavin Brown - ICANN Org: so to respond to your comment, Patrick. I don't recall

834
02:29:00.694 --> 02:29:05.689
Gavin Brown - ICANN Org: much about that discussion. The Bootstrap registry in theory does allow

835
02:29:06.197 --> 02:29:25.429
Gavin Brown - ICANN Org: names sort of higher up in or lower down in the hierarchy. To be registered into the Bootstrap registry. Because the the matching policy is is the closest in closing name. Essentially diana won't accept any registration. That's not a Tld.

836
02:29:25.550 --> 02:29:26.899
Gavin Brown - ICANN Org: That.

837
02:29:27.505 --> 02:29:32.489
Gavin Brown - ICANN Org: is perhaps a issue of practicality, because obviously it's hard to authenticate

838
02:29:32.530 --> 02:29:35.480
Gavin Brown - ICANN Org: anyone who's not a tld operator, if you're iana

839
02:29:35.887 --> 02:29:50.210

Gavin Brown - ICANN Org: but it may also be that there's a you know a a hole in the configuration that is missing because or in the policy sorry, the specification is missing. No policy specification.

840
02:29:50.706 --> 02:29:52.373
Gavin Brown - ICANN Org: Perhaps to allow that.

841
02:29:53.720 --> 02:29:56.540
Gavin Brown - ICANN Org: The the question of whether to use Serp record.

842
02:29:57.010 --> 02:29:58.230
Gavin Brown - ICANN Org: He's

843
02:29:58.710 --> 02:30:08.460
Gavin Brown - ICANN Org: problematic because of the question of boundaries and and how you define administrative boundaries in the Dns, which obviously, you know, people have tried, failed to do

844
02:30:09.058 --> 02:30:11.799
Gavin Brown - ICANN Org: and remains an unsolved issue.

845
02:30:12.846 --> 02:30:27.640
Gavin Brown - ICANN Org: Question from Olivier. What kind of adapt performance to the stealth audit service have didn't actually check so very preliminary check was just to check whether I get Json back for help. Rest. But the next step would probably be to add

846
02:30:27.680 --> 02:30:32.550
Gavin Brown - ICANN Org: checks on the content of the of the adapt conformance array.

847
02:30:35.820 --> 02:30:37.060
Gavin Brown - ICANN Org: You have another.

848

02:30:37.060 --> 02:30:38.370
Hadia Elminiawi: Supermark. Yes.

849
02:30:38.370 --> 02:30:51.940
Gavin Brown - ICANN Org: Yeah. So Mark asks commenting on the discussion that we had in the weird working group, pros and cons on each approach. Consensus was the Iina boost track registry. There you go. So so it was discussed. But the the consensus was that

850
02:30:52.220 --> 02:30:54.389
Gavin Brown - ICANN Org: Booshet registry was the better way to do it.

851
02:30:57.470 --> 02:30:59.880
Gavin Brown - ICANN Org: If there are no more questions we can move on.

852
02:31:00.290 --> 02:31:27.139
Hadia Elminiawi: Yes, thank you so much. Gavin, for this presentation, and for the discussion again, if you have more questions to Gavin, we do have some time at the end of the workshop, and now we move to Isaac Henderson, and his presentation is under the title Dns as a bridge to establish interoperable trust across different trust anchors. Isaac. The floor is yours.

853
02:31:27.370 --> 02:31:28.290
Hadia Elminiawi: Yeah.

854
02:31:28.290 --> 02:31:29.070
Isaac Henderson: Thank you.

855
02:31:30.320 --> 02:31:38.900
Isaac Henderson: Yeah. So I'll just give a short introduction. So myself, Isaac. So I'm working as a senior researcher in front of Iowa and based in Stuttgart, Germany.

856
02:31:39.020 --> 02:31:44.710

Isaac Henderson: And today my talk is going to be based on how Dns can be used as a bridge

857
02:31:45.388 --> 02:31:48.979
Isaac Henderson: to establish interoperable trust across different trust anchors.

858
02:31:50.085 --> 02:31:51.120
Isaac Henderson: Next slide, please.

859
02:31:52.100 --> 02:32:00.389
Isaac Henderson: Okay, so the agenda for the stock. So follow. So I just speak about why, it's the and the current motivation of the stock and also

860
02:32:00.885 --> 02:32:17.774
Isaac Henderson: then I introduce our technology called train. And then we also see a concrete use case where we worked on the scenario of the Guy X actually, or the data space scenario. Where have we used this and also where we also developed

861
02:32:18.150 --> 02:32:35.080
Isaac Henderson: a code base open source code base, how this can be used across federations. So that's a use case of kayaks, Federation services to build ecosystems. And then I all we also give our unified signature and verification model based on Dns, and then followed by outlook and conclusion.

862
02:32:35.810 --> 02:32:37.050
Isaac Henderson: Next slide, please.

863
02:32:38.150 --> 02:32:45.480
Isaac Henderson: So why? Why? We need to establish trust across interoperable ecosystems or trust anchors.

864
02:32:45.560 --> 02:33:00.990

Isaac Henderson: As we all know, the digital identities, and also the verification of trust is coming more and more especially, and also not only just. Yeah. Mo, moving towards a decentralized ecosystem, and especially cross domains, for example.

865
02:33:00.990 --> 02:33:25.163
Isaac Henderson: A. And how do we establish this trust, for example, in European Union we have this epsi ecosystem or udu wallet, which is the current work which is going on to establish a digital wallet for European citizens, and also, for example, the Kayx which also not only concentrates on identities of natural persons, but also on supply chain identities and device identities. And catnax, for, for example, focuses on

866
02:33:25.620 --> 02:33:43.630
Isaac Henderson: identities of automotives, and especially also the nest guidelines. For example, the domain identities we are also considering so these all identities are operated across different sectors, and the credentials will be different. And how do they speak to each other, or how they can be interoperable across each other, because, each, some, some

867
02:33:43.840 --> 02:34:09.029
Isaac Henderson: identity systems follow the blockchain approach, you know, or some follow a different decentralized nodes like ipfs, for example. But how do we establish this trust across the secret system? And how do we recognize this? The credential issued by this organization is trustworthy or not. So that's why. We are trying to show how we can bridge this anchor using Dns and how this can be effective in

868
02:34:09.400 --> 02:34:15.679
Isaac Henderson: in future for organizations to operate their own trust registries and also their trust anchors.

869
02:34:15.980 --> 02:34:17.270
Isaac Henderson: Next slide, please.

870
02:34:18.910 --> 02:34:20.539
Isaac Henderson: Yeah. So the

871
02:34:20.610 --> 02:34:27.670
Isaac Henderson: the technology. What we have developed in the past 6 to 7 years, which is called train, so which is based on

872
02:34:28.112 --> 02:34:34.167
Isaac Henderson: which is called the trust management infrastructure. So the main idea actually, for this

873
02:34:35.070 --> 02:34:48.260
Isaac Henderson: idea of train is to build trust frameworks, and also allow each and every identity or entities to define their own trust. Anchors or trustable authorities of root of trust, and also actually

874
02:34:48.780 --> 02:35:12.379
Isaac Henderson: to basically use their own ecosystem. So not only just depend on centralized ecosystem, or like, for example, like certificate authorities, or you know, or centralized fitted catalogs, for example, but rather each and everyone can manage their own databases, or you know that define their own trust anchors and policies in a more decentralized way. So for that, actually, we use this Dns infrastructure. We

875
02:35:12.702 --> 02:35:33.310
Isaac Henderson: we publish the trust list or the anchoring that of the trust list in the Dns. And we also use the Dns or Dns sec verification, so that the chain of trust is being intact. And so we provide our components, actually, which is used for administrating the trust list, for example, onboarding of members or entities into the trust list.

876
02:35:33.310 --> 02:35:55.049
Isaac Henderson: And also we have also a verify component which is used for validating the trustworthiness of the credential or anything. Maybe so, the idea what we have proposed is technology agnostic. So we are not only just depending on, for example, x 5 0 9 certificates or Pki infrastructure, but rather we also support blockchain based, and also at the same time

877

02:35:55.050 --> 02:36:07.268
Isaac Henderson: with the existing certificates, also ecosystem. So currently it has been piloted in different projects, starting from 2,016 in lightest and in the last years we worked with Ngi labs and also with

878
02:36:08.150 --> 02:36:31.190
Isaac Henderson: Yeah, companies like Huawei Sikpa, and also validated Id. And also we also did a pilot project on health credentials for Undp, and recently, also in a German showcase projects like once, and which is a digital identity project. And recently, we also did a corporation project with these systems. And in bringing this into eclipse status ecclips foundation as a open source code

879
02:36:31.680 --> 02:36:32.990
Isaac Henderson: next slide, please?

880
02:36:34.280 --> 02:36:57.929
Isaac Henderson: Yeah. So as we all know, this trust chain, so digital identities or any ecosystem might be, you know. So we have the 3 main entities. So issue a holder and verifier, for example, and the how, for example, the credentials can be issued by any different issues across the world? And, for example, how does the verifier, or, you know, can validate this credential comes from a trustworthy

881
02:36:57.930 --> 02:37:05.710
Isaac Henderson: issue of, for example, currently we all know the browser ecosystem helps us in identifying the certificate authorities, and also, you know, ensuring that

882
02:37:06.023 --> 02:37:30.186
Isaac Henderson: Domains are trustworthy, and also, for example, but when we go into more decentralized network. So then, how are we going to do it? You know. So, and also when each follow their own keys, and also not just based on Pki, but rather they have their own did based keys. So how this can work. So for that, actually, we have this approach of this governance framework. So that means any domain operator

883

02:37:30.500 --> 02:37:48.342
Isaac Henderson: can have operate this trust framework, for example. So that's what we call trust framework Manager, which is called Tfm. And the D set M is called the zone manager, actually. And so these are distributed components. So this may not be just managed by single entity, but rather any entity can manage their own trust frameworks.

884
02:37:48.650 --> 02:38:10.940
Isaac Henderson: and these trust frameworks have the option to link the trust list, and that means they'll URL of the trust list can be linked in the Dns Zone manager, actually, which sets a pointer. And this is the Ttv. Is a component which is used for validating the trust based on the policies which are assigned locally. So that means this is also a decentralized component, so that means it can. It may not be just in

885
02:38:11.260 --> 02:38:34.790
Isaac Henderson: in installed in a cloud, for example, but rather it can be installed locally based on the policies. They can have regional policies to validate the transaction. So that's how actually the it can assist the verifier and validating the transaction. But also the same component can also be used in holder, and also issue of, for example, also to validate whether this the

886
02:38:34.790 --> 02:38:53.130
Isaac Henderson: transaction which was happening from issuer to holder is going to be a trustworthy holder, for example, or before a holder gives some data to a verify it, it can also validate whether the service providers a trustworthy service provider, so that also might can be used actually. But here we just demonstrate a single use case of verify

887
02:38:53.170 --> 02:38:54.360
Isaac Henderson: next slide, please.

888
02:38:56.220 --> 02:39:19.250
Isaac Henderson: Yeah. So for this, actually, so I've just since this is a Dns community. And also I just brought, I brought us a use case based on dns, registry and registrants, for example. So how, where we can use this trust

list, because we are also moving into the NIST guidelines and also digital identities in this ecosystems. And we also had a talks on that.

889
02:39:19.607 --> 02:39:29.620
Isaac Henderson: So, for example, yeah, we have, for example, the Registry Trust List, for example, which is operated by Canori Ima, for example, where they have the registry

890
02:39:29.859 --> 02:39:41.569
Isaac Henderson: locator, for example, they operate their trust list, and they on board the trust list in their own trust framework so they can have their own governance framework, and you know, and things like that which is out of scope of the train. But it can be decided locally.

891
02:39:42.030 --> 02:39:56.060
Isaac Henderson: and every regional registrar, for example, for onboarding the registrar Trust List, you know. So for onboarding the domain operators or domain registers, so they can have their own trust list of their regions. So, for example, if the domain registry.

892
02:39:56.060 --> 02:40:13.445
Isaac Henderson: when they issue some credential to the registrar, for example, so how do they know that the credential issued by this region register is also linked to the I can, for example, right? So that's where they have that they set a pointer record. So we use the 2 point records, actually the pointer and the Uri Record.

893
02:40:13.740 --> 02:40:36.095
Isaac Henderson: where the Uri record you can ha! You can anchor different trust list, for example, of Http based URL or Dids, or you know any other ipfs links or anything it can be can be used here, and pointer is used to point across each ecosystem or trust framework, for example, because some operators they might not include, they might not operate their own trust list, but if they want to point across each other.

894
02:40:36.390 --> 02:40:46.666

Isaac Henderson: They can use the pointer records for this use case. So you might have confusion here, for example, pointers use for reverse. IP, for example. But here we use this for this

895
02:40:46.960 --> 02:41:09.429
Isaac Henderson: use case of pointing to different trust frameworks. And also we have this standardize this one actually to use, so that in order to prevent this confusion, so underscore scheme, dot underscore trust. And then comes our trust framework name actually so, by which we differentiate that the our technology uses, you know, a standardized re resource based records. And this can be

896
02:41:10.700 --> 02:41:18.190
Isaac Henderson: also known to others, and that so that it doesn't coincide with the domain names registry, or you know, the Ips, for example.

897
02:41:18.560 --> 02:41:20.090
Isaac Henderson: next slide, please.

898
02:41:20.890 --> 02:41:32.499
Isaac Henderson: So here, actually so, and we had an opportunity to look into a complex ecosystem of kayaks, actually, where there can be different ecosystem and involved across different

899
02:41:32.950 --> 02:41:54.165
Isaac Henderson: across the Guy extras frameworks. So they have and each ecosystem can have their own governance and also their own trust frameworks. That that means they are, quite flexible. And but at the same time they comply with the Guyx guidelines. So and so they had this flexibility. So that's why we had an opportunity to think about how they can use Dns, because currently, Dns is quite

900
02:41:54.460 --> 02:42:18.169
Isaac Henderson: is an anchor of trust used by any organizations. And you know, so this can be a quite useful tool for bridging ecosystems, and also ensuring the validity of credential across ecosystem, and not reissue certain credentials again, to be used in certain ecosystems so which which also can

be prevented. So that's what that's the idea which we thought about it. So to work towards a decentral, federated and interoperable ecosystem

901
02:42:18.620 --> 02:42:19.940
Isaac Henderson: next slide, please.

902
02:42:21.400 --> 02:42:42.860
Isaac Henderson: and this project was funded by a Kayak Federation Service. Kayak is a global ecosystem. So there comes a separate part of Kayak Federation services which is aimed for providing components for building federations. And these components. What are built in this part of kayaks? Federation services will be part of us published in this eclipse foundation in this source code community. Yeah.

903
02:42:43.070 --> 02:42:44.140
Isaac Henderson: next slide.

904
02:42:46.030 --> 02:42:53.284
Isaac Henderson: Yeah. So how do we address how? What role to stay train play here? Actually so train addresses the trust problem of

905
02:42:54.080 --> 02:43:15.109
Isaac Henderson: These ecosystem require a decentralized, flexible, and interoperable trust, and how the individual federations can manage their trust anchors in a sovereign way, because in when considering European Union that currently the UA. Does to regulation is coming up and Epsi have their own ledger based regulations, or you know, for example, and there are multiple other frameworks, for example, Mdoc.

906
02:43:15.110 --> 02:43:42.680
Isaac Henderson: the Us. License. They have their own framework, for example, so, and each one have their own level of assurances, and also these things are different. So how do they can speak to each other? And also how do they can interoperate together, you know so, and also managing trust is quite complex, and it is not addressed. So th those are the things which, had we had in mind so to mainly aiming towards as interoperability of

a trust framework, and also discovery of federations in a more decentralized way. So that was our aim.

907
02:43:43.490 --> 02:43:44.760
Isaac Henderson: Next slide, please.

908
02:43:46.430 --> 02:44:02.510
Isaac Henderson: Yeah. So these are the choir train architecture or the components we have actually. So, as I mentioned, the Tfm is responsible for operating the trust list. And they have specific api endpoints, actually, which is used for which can be used for notarization. Or you know, any other

909
02:44:02.510 --> 02:44:26.900
Isaac Henderson: component which is responsible for enrolling the entities, or, you know, members, into this Federation of the Trust list, and this one, this link is the trust framework manager, URL, or the trust list. URL is linked in the Zone manager. So zone manage Dns zone managers, we all know. So this one is operated by the company, for example, and they have their zone file, and this zone file is universally discoverable, so that, as I mentioned, the underscore scheme

910
02:44:26.900 --> 02:44:37.290
Isaac Henderson: trust this file will be universally available in this zone zone file, and the companies or the entities who wants to validate, you know, so that there's a Ttv. As I mentioned, is used for the validation.

911
02:44:37.670 --> 02:44:46.460
Isaac Henderson: and the Dns resolver uses the Dns, commands the trust framework names to locate the trust list and then find out whether the

912
02:44:46.710 --> 02:45:06.989
Isaac Henderson: entity which is issued. The credential is there in this trust list or not so, by which, they can verify this entity is trustworthy or not so here we have different interfaces for Eps and open id Federation. You can have different interfaces. And also we can also have did resolvers or any other resolvers built into this component.

913
02:45:08.280 --> 02:45:16.759
Isaac Henderson: So basically, our Ttv supports external verification of trust. And this can be easily integrated into verifier or tsa based on libraries or Apis

914
02:45:17.280 --> 02:45:18.700
Isaac Henderson: next slide, please.

915
02:45:19.980 --> 02:45:46.239
Isaac Henderson: Yeah. So this is a gayx component as we developed. Actually. So this is similar model which I showed. But Button Gayx, we had a 3 step process because a compliance ecosystem. And then comes a federation. And then comes an organization perspective, so each can operate their own trust list. So here we also created a unified trust model, actually, which is based on dit. So we don't. We not only exhibited with a normal Https, URL, but rather we also use the

916
02:45:46.240 --> 02:46:10.080
Isaac Henderson: used to did document. And then actually, we also used this trust list to develop a unified trust model. And how this can be located across each other. And then, you know, and this was a major task of this project. I'll actually so by which any trust list, and any different formats can be wrapped into a verifiable credential, so that it can be globally verified and unified, unif unifiedly verified, so that it is not.

917
02:46:10.080 --> 02:46:16.919
Isaac Henderson: You need not have interfaces for Xml or Jason, for example, but rather you just verify proof in a form of verifiable credential. Yeah.

918
02:46:18.500 --> 02:46:30.130
Isaac Henderson: So that is the idea. And then, for example, here, for example, when the Organization Trust Federation, they have the pointer set in their zone file, and then the Federation also trusts the pointer, the Guyx compliance

919
02:46:30.240 --> 02:46:31.450

Isaac Henderson: next slide, please.

920
02:46:33.230 --> 02:46:55.600
Isaac Henderson: So here we. This is an example of a trust list. So we have developed a trust list based on, inspired from the address version one. So where they have different details of a trust service provider information, for example, for here there's an automotive use case. And then there's a different each service provider can have multiple services. So one can issue some credential. Another can issue responsible for some services.

921
02:46:55.600 --> 02:47:18.520
Isaac Henderson: And you know. So that that's why we have this distinction of a Serve Tsp name. And this is a service provider. And this can host multiple services in it not only assurance, but also verifications and validation stuff. So that's why. Here the service stop. Identifier is a place where we issue our Id is being written. So this is here we have it. But it can also be a normal Http, Uri or Dns name included over there.

922
02:47:18.940 --> 02:47:20.209
Isaac Henderson: Next slide, please.

923
02:47:21.800 --> 02:47:51.720
Isaac Henderson: Yeah. So here we exhibited how this can be verified in digital identity. So we use this anchoring in this trust in the, in the verifiable credential and tested it. So we use the terms of use, attribute and of the verifiable credential data model one dot 0. And here we included in the trust scheme. The Dns names actually. So that means if we don't specify, for example, the trust list directly in the trust trust and the verifiable credential, but rather we specify the name of the trust framework. For example.

924
02:47:51.720 --> 02:48:09.539
Isaac Henderson: as I mentioned in the red box here you have a note in this trust team belongs to notary and compliance, and then this detail will be later fetched at the verifier side will be used to validate, but that this issuer, whatever this did. Key is part of this trust framework or not, that will be verified, verified, and validated.

925

02:48:10.740 --> 02:48:12.050
Isaac Henderson: Next slide, please.

926
02:48:13.470 --> 02:48:36.890
Isaac Henderson: Yeah. So these are the so in the Ttv side. Actually, we require these 3 main components. So we don't require much information, and our policy will be responsible for validating and finding out whether this issue is present in this trust framework. So you can have multiple array of trust scheme pointers based on Dns names. And it can also go across multiple Dns or Multiple Trust lists and verified whether this entity is there or not.

927
02:48:38.560 --> 02:48:39.850
Isaac Henderson: Next slide, please.

928
02:48:40.860 --> 02:48:47.279
Isaac Henderson: Yeah. So this is the unified signature model which I mentioned. So this is, provides a little bit of detail in it into it.

929
02:48:47.280 --> 02:49:09.329
Isaac Henderson: based on did so in the Uri. You not only anchor http, Uri, but rather it did web. And then, which has a did document. As we all know, this can be in a blockchain, or it can be also in a normal web server, and then it has a verifiable credential which points to the Guy X Trust list the trust list. So by which you don't have any signatures for each and every trust list in a separate way.

930
02:49:09.655 --> 02:49:22.040
Isaac Henderson: But rather, we have a uniquely representation form of yeah, the PC data model, actually. And so that is, that's why it can be easily verified and across globally and also uniquely in a more user friendly way.

931
02:49:22.990 --> 02:49:24.269
Isaac Henderson: Next slide, please.

932
02:49:25.210 --> 02:49:50.929

Isaac Henderson: Yeah. So these can be integrated. So what are the components which you have developed so can be used, helpful for the validating the trust, and not only validating trust, but also it can be used in the wallet to verify, for example, the validity of the service provider before giving any data to them, and also it can be used in the notarization services. That means in the onboarding process to enroll some entities into the trust list. But thereby you can validate and also

933
02:49:51.198 --> 02:50:00.851
Isaac Henderson: verify that this entity is trustworthy or not. So the so our components can be integrated in different levels and use be used for validating the trust in different purposes. Actually. So that is the idea.

934
02:50:01.700 --> 02:50:03.049
Isaac Henderson: Next slide, please.

935
02:50:04.290 --> 02:50:27.170
Isaac Henderson: Yeah. So so by which we provide an approach, and also a technology which can be used across diverse ecosystem by using the Dns, that which is mostly flexible, and also, you know, which is also quite decentralized. We offer a flexible trustworthy approach to operate interoperable trust across different trust anchors and the unified trust model can be also helpful. So there's

936
02:50:27.200 --> 02:50:43.399
Isaac Henderson: a in validating and and also the trust lists across different formats. So we tested in Xml and Json format. But it can also be used for other different formats if anything is available. Actually. And currently, we are also looking to test and also

937
02:50:43.720 --> 02:50:45.930
Isaac Henderson: testing other test beds. Actually

938
02:50:46.740 --> 02:50:47.740
Isaac Henderson: next step.

939

02:50:49.000 --> 02:51:18.290
Isaac Henderson: So this is my last slide. So the the currently we are looking into how to standardize this approach actually, not only for natural person identities, but also for mission identities and supply chain use cases because we believe that those verification and validation become complex. And we are also currently doing with the Unp as a global pilot for health use case. And also currently, we are also planning to evaluate, not only with the Dns name server, but also with the ethereum name service, and also, for example.

940
02:51:18.562 --> 02:51:24.557
Isaac Henderson: Gnu name system, which is also based on the Rfc draft. Actually. So we are also planning to integrate with them and

941
02:51:24.830 --> 02:51:39.266
Isaac Henderson: verify how this can also be flexible and use across name services of other ecosystems. And currently, we are also planning to implement the Open Id Federation Trust List and Epsil Trust us issue, issue, issue, issue a registry as an interfaces into a T-TV

942
02:51:39.846 --> 02:51:57.560
Isaac Henderson: but it's it's in the process. And we are planning to do it. And yeah, if if there are inputs, how this can be standardized, and I can or like, you know, itf I'd be, I'd be happy to get to know some contacts or working groups relevant to it. And currently the source code of all these different components are available is open source code in the

943
02:51:57.930 --> 02:52:05.259
Isaac Henderson: following link, and you can have a look into it. And if you have any doubts, yeah, I'm happy to answer the questions and thank you. Next slide

944
02:52:06.920 --> 02:52:07.670
Isaac Henderson: perfect.

945
02:52:09.640 --> 02:52:15.219

Hadia Elminiawi: Thank you so much, Isaac. This is Hardia for the record, and we have a hand from Simon.

946
02:52:15.420 --> 02:52:17.460
Hadia Elminiawi: Simon. Please go ahead.

947
02:52:18.060 --> 02:52:30.580
Simon Fernandez: Great thanks, thanks a lot for the presentation. Most of the systems, the identity systems that you describe are pretty conservative, conservative when they are counting the

948
02:52:34.250 --> 02:53:03.730
Simon Fernandez: trust occurred in your system. You are adding an additional trust point like the Dns sector system. Do you think the the identity management systems would actually be okay with adding this new point of failure where you have to trust the root certificates of the Dns or the root or the Dns certificates of your of your name, server.

949
02:53:04.810 --> 02:53:15.400
Isaac Henderson: That's a good question. Actually, so, this is an optional part. Actually, because we have this option when someone wants to validate the chain of trust, because you know the Dns as a normal, it can be

950
02:53:15.400 --> 02:53:38.959
Isaac Henderson: spoofed or changed on the man. It is prone to the man in the middle of the attack. But, Dns, sec. Off this complete chain of trust. And and I know actually not. All organization have this Dns sec implemented. So that's why we? We are flexible. Actually, the Dns sec. Is for level of assurance high, I would say, for example, but you don't need to have it as a mandatory, for example. So we also function without that feature of Dns. Sec. Also actually.

951
02:53:41.820 --> 02:53:57.150
Simon Fernandez: Like, even with the Dnssec enabled, you still have to have those root certificates of the Dns chain to trust as to use as anchors for those Dnssec chains of trust.

952
02:53:57.630 --> 02:53:59.020
Isaac Henderson: Yeah, exactly.

953
02:53:59.260 --> 02:54:03.469
Isaac Henderson: But that is done by the Dns valid resolver or the validator. Right?

954
02:54:03.950 --> 02:54:13.960
Simon Fernandez: Okay, so you have to put additional trust, like you have to trust your Dns resolver in order for this system to deploy its whole power of certification.

955
02:54:13.960 --> 02:54:26.749
Isaac Henderson: Exactly. So you can say, Okay, I trust only certain resolver, for example, and not all the resolver. So by which you can also make restrictions and make your system, you know, in a certain direction, for example. So that's also possible. Yeah.

956
02:54:27.330 --> 02:54:28.789
Simon Fernandez: Okay, thanks a lot for your answers.

957
02:54:30.445 --> 02:54:44.309
Hadia Elminiawi: Thank you, Simon. And Thank you, Isaac. So we have a question in the QA. Pod from Jim, he says, could this be leveraged to set up a trust list of verification? Providers in support of an is 2.

958
02:54:45.360 --> 02:55:12.530
Isaac Henderson: Yeah, I think it is definitely possible. Actually, so we can definitely build such things. Actually. So that's why I also brought up a use case, how this can be used for verifying the registrars, for example. And I think definitely this can be used actually. So if we we are flexible with the data model. And I'm happy to suggest some use case or the data model what we have. And then we can adapt it based on the flexibility or the requirements of the needs to. For example. So yeah, we can do that.

959

02:55:15.380 --> 02:55:43.529
Hadia Elminiawi: Thank you, Isaac, and I don't see any more questions in the chat. I don't see also any hands up. So. I I thank you again, and I guess now we can move to our next presenter Warner stop from Core Association. His presentation is under the title Standardized Dns signed as at a station at the stations for support.

960
02:55:49.740 --> 02:55:53.010
Hadia Elminiawi: Oh, Warner, the floor is yours.

961
02:55:53.190 --> 02:55:53.820
Werner Staub: Yet.

962
02:55:54.080 --> 02:56:01.150
Werner Staub: Okay, okay, thank you very much. I'm going to do the 1st part of this presentation

963
02:56:01.170 --> 02:56:08.600
Werner Staub: in the on the slide. And then, you know, depending on time. It do show some of the things directly kind of in a demo mode

964
02:56:08.820 --> 02:56:10.689
Werner Staub: pasting a pilot that we have.

965
02:56:11.164 --> 02:56:33.009
Werner Staub: I might brief present myself. I work for Core Association, which runs a couple of registry systems, you know, for itself and for community based Tvs. One of them is the dot sport Tld, which, is run by the International for the Associations. You know, the umbrella organizations of the International Sports federations.

966
02:56:33.140 --> 02:56:56.260
Werner Staub: and in that context. Of course, we were also exposed, and to to the, you know, difficulty of actually showing that that a certain domain is credible. You know the Dtl. D, as such, is, of course, very useful, and it is

highly verified if you look at that sport, but there is usually not much to know about it. If you go to the next slide, please.

967
02:56:57.590 --> 02:57:15.960
Werner Staub: Okay. So we came up with the idea that about the station. Just briefly say, this is not just to mitigate harm. It is also about creating value, and if you talk about mitigating harm, it is not just what we see now, because everybody knows that we have to brace for large scale use of AI to do fakes.

968
02:57:16.684 --> 02:57:33.969
Werner Staub: If we talk about creating value, you know, there is actually quite a bit of value in people being able to show that they're different from a fly by night. Website that would impersonate anybody's identity just by copying the logo next slide, please.

969
02:57:37.720 --> 02:57:44.309
Werner Staub: Okay, what do you see? Here is an actual case of you know.

970
02:57:44.890 --> 02:57:52.830
Werner Staub: complaint that came to us from one of the International Federation. It was the Orienteering World Orienteering Federation.

971
02:57:52.910 --> 02:58:05.399
Werner Staub: and what they say is that, their website and their contents being copied by people, you lose totally irrelevant domain names. Unfortunately, the resolution doesn't show what the domain name is here. It's a

972
02:58:06.053 --> 02:58:18.960
Werner Staub: I didn't think of of testing testing that. It's a a totally irrelevant domain name. It is actually on the archive.org. You can find that on the way back machine.

973
02:58:19.200 --> 02:58:36.959

Werner Staub: And it's it shows that you know, the actual content which is the content stream delivered by the Federation is used by these people, who in this particular case are trying to misuse that to place ads or to poison the search engine so that the ads can be placed

974
02:58:37.609 --> 02:58:40.809
Werner Staub: for betting websites

975
02:58:41.325 --> 02:58:52.719
Werner Staub: take down, for such a thing is hopeless, you know, there's so many of them, and you know, copying the stuff copying the the Logos is absolutely no problem. And most importantly.

976
02:58:53.020 --> 02:58:58.189
Werner Staub: the targeting by which this is actually directed at victims is

977
02:58:59.010 --> 02:59:03.089
Werner Staub: is very smart, so most of the time, you know the

978
02:59:03.280 --> 02:59:04.590
Werner Staub: the

979
02:59:05.060 --> 02:59:11.979
Werner Staub: the object of malicious impersonation will not even learn about it, because it's too well targeted. Next slide, please.

980
02:59:14.540 --> 02:59:20.710
Werner Staub: Here is just a series of things I've seen myself, but all of these come from Youtube.

981
02:59:21.120 --> 02:59:26.760
Werner Staub: And so those are sponsor links in in Youtube.

982
02:59:26.870 --> 02:59:32.170

Werner Staub: Each one of them displays not only real existing media.

983
02:59:32.610 --> 02:59:43.509
Werner Staub: but also, you know. In your second case, in the middle we see this is, you know, an athlete being targeted. You. You can see if you speak German, that you know. The obviously the translation of the the

984
02:59:44.020 --> 02:59:46.270
Werner Staub: beating text was A

985
02:59:46.300 --> 02:59:54.949
Werner Staub: was done by what was artificial. So they they got the gender roles. You know this not a foose. Para. It's fus palerin in German.

986
02:59:55.000 --> 03:00:07.839
Werner Staub: And if it's a lady, so but that doesn't matter. You know, they actually also manage to target this specifically to people who do not speak the language in which the artist is a is a

987
03:00:08.604 --> 03:00:13.210
Werner Staub: displayed as a primary, as a as a 1st language next slide, please.

988
03:00:16.336 --> 03:00:19.369
Werner Staub: What is quite relevant here

989
03:00:19.500 --> 03:00:37.010
Werner Staub: is the fact that this is a verified advertiser. I mean this specific case. All these things belong together. That's 1 series of things. The 1st element is what Youtube displays. You know, it shows a public, you know, government building in Switzerland. It's actually the Federal government.

990
03:00:37.140 --> 03:00:50.729

Werner Staub: So pretending that this is news from the Federal Government, then it says that there is, you know, something about, you know, from from TV. So basically it. It shows the one of the media outlets, 20 min, and so on.

991
03:00:50.780 --> 03:01:07.380
Werner Staub: And then, you know, if you look at the advertising advertiser center, you know, that's displayed by Google. It actually says Advertiser identity verified by Google. It also says that this organization is in Poland.

992
03:01:07.500 --> 03:01:09.300
Werner Staub: And and

993
03:01:09.860 --> 03:01:22.619
Werner Staub: of course, this identity. Verification was not based on the outgoing domain name that was associated with the ad that was presented to the to the user.

994
03:01:22.800 --> 03:01:27.979
Werner Staub: which is probably one of the things that we could help with the project I've been describing here

995
03:01:28.200 --> 03:01:29.320
Werner Staub: next slide, please.

996
03:01:30.960 --> 03:01:42.540
Werner Staub: Okay, it's just apparency, you know. People often say that you know, there should be Logos, a logo program that would actually be controlled. And to make sure that you know, we know that the site is verified.

997
03:01:42.670 --> 03:01:47.559
Werner Staub: This is actually turned out to be increasingly the wrong, you know, solution

998
03:01:47.690 --> 03:02:07.040

Werner Staub: almost harmful, actually, in most cases, because the Logos are too easy to to to copy and take down. That used to be to deterrent 25 years ago. Of course, nowadays isn't. Take. The isn't the deterrent anymore. So you know, it can be used anywhere at no cost there, almost no cost by the pirates next slide.

999
03:02:09.380 --> 03:02:17.939
Werner Staub: Okay, so the idea is to kind of use the Dns to provide verifiable

1000
03:02:18.862 --> 03:02:20.820
Werner Staub: were verified attestations.

1001
03:02:21.050 --> 03:02:24.319
Werner Staub: Let's say they, at the stations that are as verified as the

1002
03:02:24.530 --> 03:02:31.679
Werner Staub: as the credibility of the tester is verified, so we do not click.

1003
03:02:31.910 --> 03:02:48.319
Werner Staub: Proposing to send any cryptographic information along with the the statement, however, we would suppose that is signed by Dns. Sec. So if you look at the Dnsc signed, you know clearly, is the existing relationship. That would be the subdomain. Everybody knows how to wear. How this works.

1004
03:02:48.320 --> 03:03:08.259
Werner Staub: so that is usually, you know, can be totally made verifiable by Dns. Sec. In the sense that you know that subdomain.example.com can only have in created by the parting control of example.com. If it is signed by Dns sake.

1005
03:03:08.440 --> 03:03:19.949
Werner Staub: Now, in the case that we try to do, we kind of have to make some detours. So I'm taking some real examples here. Gymnastics dot sport. That's the International Gymnastics Federation.

1006
03:03:20.530 --> 03:03:33.910
Werner Staub: FIG. And the the main on the bottom, which is quite cryptic, is actually the abbreviation of the Swiss Gymnastic Federation, you know, 1st in German and then in French. You know the 2 of them together are their domain. Name

1007
03:03:34.433 --> 03:03:40.410
Werner Staub: is not maybe the most memorable memorable domain name, but quite, you know, quite effectively used.

1008
03:03:40.500 --> 03:03:50.539
Werner Staub: So what we essentially suggest is we use intermediary and Dnssec assigned domain names to do that. Can you go to the next slide, please?

1009
03:03:52.730 --> 03:03:57.050
Werner Staub: So the domain names are actually using to link gymnastics, dot sport.

1010
03:03:57.150 --> 03:03:57.860
Werner Staub: and

1011
03:03:57.980 --> 03:04:00.940
Werner Staub: the Stv. Dash. fsg.ch.

1012
03:04:01.370 --> 03:04:02.570
Werner Staub: Is one

1013
03:04:03.090 --> 03:04:05.670
Werner Staub: which is, you've seen all the on the

1014
03:04:05.990 --> 03:04:07.170
Werner Staub: left

1015
03:04:07.360 --> 03:04:09.379
Werner Staub: underscore references dot

1016
03:04:09.390 --> 03:04:22.740
Werner Staub: the domain name txt. It's a txt record, and it just points, you know, in in the form of a txt record to the domain gymnastics or so. But it doesn't even bother. Let's say, to say that this is a

1017
03:04:22.810 --> 03:04:46.410
Werner Staub: this is, you know, a C name, or anything like that because it could be more than one, it's just a text string and say, sources of at this station can be shown here. This is a mere claim it doesn't even require the in a secure. You can just put this in a normal Dns and Dns txt record and say, no. My references are those people, you know, you'd identify them by their domain names.

1018
03:04:46.600 --> 03:04:51.389
Werner Staub: And you might actually just separate the domain names by blanks. If there, if there's more than one domain name.

1019
03:04:51.620 --> 03:05:00.580
Werner Staub: And of course, what comes back once you verify that is another domain name. You see that it's a long domain name. It starts with what you see in red.

1020
03:05:00.630 --> 03:05:11.289
Werner Staub: you know. Stv. Dash, fsc.ch. Dot, and then we have a separator label. We use the name, the the label statement by to make it kind of human readable.

1021
03:05:11.620 --> 03:05:20.389
Werner Staub: Dot gymnastics dot sport, you see, as actually be doing a juxtaposition of 2 domain names which is separating them by a label in the middle.

1022
03:05:20.850 --> 03:05:23.639
Werner Staub: And it's also txt record.

1023
03:05:24.660 --> 03:05:32.610
Werner Staub: And and here comes the difficult part. We need some kind of a standardized thing that can be inside of that text.

1024
03:05:32.640 --> 03:05:49.689
Werner Staub: So we've been going to and fro with a number of ideas you know about this. Here is one of the ideas, you know, it's not possible, not necessarily the one that's going to be used in the project. But here is how it what it could look like, you know, it would say, holder of

1025
03:05:49.900 --> 03:05:57.249
Werner Staub: the holder, of being a keyword, so to speak. Gymnastics board recognizes again a keyword.

1026
03:05:57.370 --> 03:06:01.829
Werner Staub: There's a space missing. I just realized. Here it was deleted. And then in my editing.

1027
03:06:01.920 --> 03:06:04.410
Werner Staub: and Stbb. Fsg,

1028
03:06:06.410 --> 03:06:08.030
Werner Staub: the.ch.

1029
03:06:08.190 --> 03:06:08.960
Werner Staub: As

1030
03:06:09.200 --> 03:06:10.800
Werner Staub: which again is a keyword

1031

03:06:11.000 --> 03:06:26.110
Werner Staub: Member International Federation, which would be a text then, you know who's meaning would be standardized by the source of at the station. So this assumes that gymnastics dot sport would have, you know, you know, and

1032
03:06:26.160 --> 03:06:29.400
Werner Staub: a keyword such as recognizes. We call that a verb.

1033
03:06:29.460 --> 03:06:35.939
Werner Staub: and it would have you know these were in the what it actually has, and about what kind of

1034
03:06:36.110 --> 03:06:57.469
Werner Staub: thing a party might be recognized as it could be Member International Federation. It could be accredited sponsor on the or whatever those would be, up to the party. That is the source of the at the station, and you can see the source of the attestation quite clearly, because statement by

1035
03:06:57.570 --> 03:06:58.410
Werner Staub: Dot.

1036
03:06:58.760 --> 03:07:04.490
Werner Staub: that domain name is the source of the of the at the station. Can we go to the next slide, please?

1037
03:07:07.080 --> 03:07:15.720
Werner Staub: Okay, so I'm placing this in a context of where we try to start you doing this, then this is the context of the the

1038
03:07:16.040 --> 03:07:17.739
Werner Staub: international sports

1039
03:07:17.750 --> 03:07:22.290

Werner Staub: umbrella organizations. This has been recently, recently recently reformed.

1040
03:07:22.370 --> 03:07:39.869
Werner Staub: And then so you have 4 type specific umbrella organizations that that they're shown here. Those 2 together are, you know, they joined forces in another association, which is called sport accord, which also happens to be the registry operator now of the of that sport.

1041
03:07:39.950 --> 03:07:58.510
Werner Staub: But that sport is not actually central to this. This works for for any tld, or you see that below in your behalf and met there is, you know, federations. They are part of one of those, if they're you know, they're internationally recognized and on a on a high level.

1042
03:07:58.845 --> 03:08:13.679
Werner Staub: As not all the Olympic sports are always the same, so there may be changes, and on the on the regular basis in the in this, even if the regist, if the Federation has been very old, can we go to the next slide, please?

1043
03:08:15.780 --> 03:08:41.380
Werner Staub: So here is a this a use of attestations, you know, in this 1st time, just to kind of display how this works, and if he, if you go to visit the the domain name, you know the URL on the bottom. That would actually show this, you know, if in if in the one events on there, and it automatically generates the picture that is shown here

1044
03:08:41.400 --> 03:08:49.309
Werner Staub: what we see here, Jim. Wo! That's the Gymnastics Federation of the Swiss canton of woe. That's just here, close to here, not close by here to Geneva.

1045
03:08:50.297 --> 03:09:10.580
Werner Staub: then you've got the National Federation on the top. You've got the Gymnastics Federation further up. And then basically we can can have a route. of this route of at the station. That might be support the court.

Of course we might use some other resource when we actually deploy then the project.

1046
03:09:11.233 --> 03:09:19.396
Werner Staub: The idea is that of course, you know, the user might. And if a user visited this, they might get some help to interpret this. But,

1047
03:09:19.740 --> 03:09:26.270
Werner Staub: We should possibly look at where this comes from in terms of Dns. Can we go a little bit further next slide, please.

1048
03:09:28.627 --> 03:09:34.522
Werner Staub: I, just for the record showed these organizations that involved in the in the above, in the above

1049
03:09:35.720 --> 03:09:38.009
Werner Staub: that's their websites next slide, please.

1050
03:09:40.290 --> 03:09:59.830
Werner Staub: So the statements used are 2 pages statements. They're not going to go into details with them. It's just, you know. If if you look at the slides, you know, you can look at the hole. The word, or is actually clickable. You would go and see. You'd be able to see the txt records on on on Google Toolbox, which is, shows what the what has been placed there.

1051
03:09:59.890 --> 03:10:03.440
Werner Staub: And you can also see the source code, that of of the

1052
03:10:03.480 --> 03:10:05.429
Werner Staub: of the the

1053
03:10:06.110 --> 03:10:10.051
Werner Staub: page that whose link was there before next slide, please.

1054

03:10:10.710 --> 03:10:11.590
Werner Staub: And

1055
03:10:13.950 --> 03:10:24.230
Werner Staub: so that's the second page of those you know. You see, this is about, you know half, and you know, a little bit more than half a dozen attestation or report and statements.

1056
03:10:24.350 --> 03:10:36.119
Werner Staub: We came to a conclusion that would be different. Kinds of statements used to actually make a valid at this station, and one of the approaches was to say to some of the attestations, some of them reports, and some of them claims

1057
03:10:36.320 --> 03:11:02.680
Werner Staub: going into deep details is probably not important. You know. The essence is that just like when you send the Cv. To someone the Cv. Might actually contain references. And you know we tell the numbers of people to call who might be able to, you know, attest to, you know the credibility. Of your Cv. You've got the same logic here in the form of claims, in the, in the reference attribute leave.

1058
03:11:02.750 --> 03:11:05.529
Werner Staub: or in the form of report statements

1059
03:11:05.970 --> 03:11:07.320
Werner Staub: and go next slide, please.

1060
03:11:09.490 --> 03:11:12.610
Werner Staub: Now the difficulty is the language.

1061
03:11:12.780 --> 03:11:41.899
Werner Staub: you know. Say we, we were wondering, you know, how can we make it such that he would actually have enough traction. And of course sport is powerful. You know there's many reasons to look at what the Sport Committee has to say about its participants. It can go from a number of at

this stage. Central, you know, trust anchor like places to individual domain names on held by clubs or

1062
03:11:42.586 --> 03:11:43.919
Werner Staub: or by

1063
03:11:44.770 --> 03:12:05.080
Werner Staub: or by even athletes, or or or teams. That. That is actually not so much the the problem to find, you know, and these these records we have the advantage that you know, if they're there. No, they're easy to to to look up now that even on a web browser, we can actually just

1064
03:12:05.080 --> 03:12:16.821
Werner Staub: query, one of these online resolvers, who will actually check in the Dns sake. So we don't even have to bother about whether you know Dns, sec is

1065
03:12:17.270 --> 03:12:23.619
Werner Staub: is always there so long as we look at the term at the top and at the stations.

1066
03:12:24.329 --> 03:12:33.840
Werner Staub: Now, if you make it just for sport, it will probably not have enough traction, so we should find a language that could be used elsewhere as well.

1067
03:12:34.070 --> 03:12:38.320
Werner Staub: And you know so. But you see 2 examples here.

1068
03:12:38.824 --> 03:12:46.429
Werner Staub: But you see also, in these examples we try to make. We need to try to make sure that it is similar to natural language.

1069
03:12:47.060 --> 03:13:01.390

Werner Staub: So we have a Dns record that could be displayed somewhere. But if you make this cryptive? Ask, for instance, Deacon or Spf, or you know they're really hard to understand, you know, if you show this to a lawyer, the lawyer will say, Oh, Aina, I defer to our techies

1070
03:13:01.630 --> 03:13:08.970
Werner Staub: this is not something that we could have. You know, the the the in-house lawyer of a certain company would have to be quite comfortable

1071
03:13:09.000 --> 03:13:18.319
Werner Staub: that they know what they're doing here. So so it should be a simple, a simple language. But it should still be computer readable.

1072
03:13:18.850 --> 03:13:34.419
Werner Staub: And now there is, there is, you know, history in in it of doing English like syntax and sexual is one of those cases, and we might also have an a new reason. To use English like syntax

1073
03:13:34.420 --> 03:13:56.720
Werner Staub: is the fact that you know some, engines will use natural language processing to kind of make sense of things that they haven't, you know, actually programmed into their into to their capabilities. That's maybe not yet a concern, but might be, you know, an opportunity in the future what you see in the in terms of those examples. You know, I take those, as you know, a typical example of a missing at this station.

1074
03:13:57.040 --> 03:13:59.769
Werner Staub: This is like an attestation that should exist

1075
03:14:00.211 --> 03:14:21.048
Werner Staub: everybody you know who is, you know, computer Literate knows that office.com is is owned by Microsoft, and you know the same people also know that no machine knows about the fact that office.com is is is owned by by Microsoft. So making this clear is actually quite quite straightforward and

1076
03:14:21.510 --> 03:14:32.510
Werner Staub: and in the same way. You know, we could have attestation statement by rating agencies, you know. Yeah, this year where you see the thing called clear Prudence. It's just a pilot idea.

1077
03:14:33.180 --> 03:14:42.650
Werner Staub: It's it can say that it knows microsoft.com as a well known brand. And so the term the methodology would be up

1078
03:14:42.650 --> 03:15:03.300
Werner Staub: to to this to this party. If somebody wanted to set set up a rating agency or rating diploma Mill dot Company group, you know they could do that, you know, nobody would take them seriously. It wouldn't do any harm, and because people who use this would know why they, you know, they place their trust anchors respectively. Next slide, please.

1079
03:15:07.660 --> 03:15:10.230
Werner Staub: Is it is the next slide? Or is that just that last slide?

1080
03:15:16.240 --> 03:15:24.520
Werner Staub: Okay, so so this is the last, I think so. We you know, the the one that you see that is currently live

1081
03:15:24.750 --> 03:15:33.280
Werner Staub: is an experimental project we started about a year ago, and that is what we using now to start a project with with the sporting in order to gain some experience.

1082
03:15:33.380 --> 03:15:35.199
Werner Staub: And we and

1083
03:15:35.582 --> 03:15:44.020
Werner Staub: we saw that, you know some things, you know that. That would probably be a good idea, and some of them might be a bad idea.

1084
03:15:44.100 --> 03:15:55.720
Werner Staub: probably the the the one that you see in the bottom, you know the trust keywords, you know. That we start was a good idea. In the beginning

1085
03:15:55.750 --> 03:16:04.609
Werner Staub: we came to the conclusion, that's a bad idea. It's just too broad, you know. If you have an attestation, says, you know rating agency, such and such trust

1086
03:16:04.870 --> 03:16:11.459
Werner Staub: the bank, such and such. It doesn't mean that the bank is so, you know, is is liquid and able to repay. It's a it's a

1087
03:16:11.520 --> 03:16:28.380
Werner Staub: it's deposits. That is not what it means it means that it is. It is a major brand. So we shouldn't use trust, probably in this. And so we are looking at the idea of saying that, you know, using a keyboard like nose as and that's probably would be would be used in the

1088
03:16:28.910 --> 03:16:32.989
Werner Staub: in the, in what we use for the for the sport.

1089
03:16:33.200 --> 03:16:36.427
Werner Staub: and they we probably would use, you know, kind of

1090
03:16:38.690 --> 03:16:42.410
Werner Staub: These split verbs like recognizes object

1091
03:16:42.550 --> 03:16:54.369
Werner Staub: as an National federation. There is also the question of whether we use, you know, the clarifying, and you and the elements, such as holder of.

1092

03:16:54.620 --> 03:17:01.769
Werner Staub: you know, gymnastics that sport rather than just saying, gymnastics does sport. That is the International Gymnastics Federation.

1093
03:17:01.780 --> 03:17:12.420
Werner Staub: You have to say, holder of gymnastic sports word and make it possibly clear, you know, for you know the legally suit that is not quite the same concept.

1094
03:17:12.570 --> 03:17:23.970
Werner Staub: but then it is, so long as they make it a relatively simple language, it it should work. Now, the rest here is maybe, you know, you know, depending on how much time we have.

1095
03:17:23.980 --> 03:17:26.499
Werner Staub: Just maybe one thing, as long as we look at this slide.

1096
03:17:26.540 --> 03:17:38.420
Werner Staub: I would very much be interested in opinions and help for the language that we, you know, try to roll out by the second half. You know the middle of the second half of

1097
03:17:38.580 --> 03:17:55.580
Werner Staub: of of this year, so as to start the project for dot for the the sport community. In January next year we actually went ahead, and, you know, propose an I can grant request. And for this, not for the technical stuff. That is the easy beat

1098
03:17:56.060 --> 03:18:07.676
Werner Staub: did did the hard bit is the promotion of the best practice. Zoom to do so it will be, we need to get, you know. Go, you know, use the existing, the existing

1099
03:18:08.730 --> 03:18:28.750
Werner Staub: relationship. That sport accord. You know, the association of the Umbrella Federation has. And this is actually quite a significant effort to

standardize. On the one hand, the language to do those at the stations, and, on the other hand, of course, make sure that there is traction that there's enough participants who do this so that

1100
03:18:28.750 --> 03:18:41.740
Werner Staub: a party like Youtube would be able to see that. You know, if it's port, there will be, there will be attestations, and there will be an ecosystem where they can find in the in web of trust logic.

1101
03:18:41.770 --> 03:18:48.570
Werner Staub: a place where it could be quite, and I'm sure that you know they they they know that

1102
03:18:48.790 --> 03:18:51.030
Werner Staub: given domain name is credible

1103
03:18:51.870 --> 03:18:58.379
Werner Staub: if I can. Just briefly they take the screen. The the shared screen is that, oh, I have that available.

1104
03:18:59.340 --> 03:19:01.300
Werner Staub: Okay, share.

1105
03:19:01.900 --> 03:19:03.450
Werner Staub: So and

1106
03:19:05.250 --> 03:19:06.700
Werner Staub: we're using this.

1107
03:19:06.830 --> 03:19:12.250
Werner Staub: Okay, what you see here is the is the the screen for

1108
03:19:12.668 --> 03:19:30.290

Werner Staub: that I mentioned. So you know, on hover. It would show the the actual cases, and it goes a little bit further than just pre providing at the stations. For instance, if you let's just do a reload. It has some some of the stuff that doesn't come immediately.

1109
03:19:30.290 --> 03:19:47.660
Werner Staub: if you and if you look at the second thing is, it talks about legal entity identifiers. You can click on those. And you see, for instance, the records, you know, of the legal entity identifier of of the International Gymnastics Federation.

1110
03:19:47.660 --> 03:20:11.899
Werner Staub: You know, the the user interface would be something to to work on. That does not matter really what I mean. Anybody can come up with the user interface for this. The whole point is that, you know, which is to illustrate what could what could be done with with at the stations? You also see that the trust verb here is the one that we think is probably not the the greatest idea. So we probably change that.

1111
03:20:12.030 --> 03:20:18.919
Werner Staub: The other thing that you know probably want to change is that you know the language that it describes how, what the relationships are.

1112
03:20:18.950 --> 03:20:44.484
Werner Staub: So this probably is too short. It is not clear, you know, it has as international federation in this cryptic way would not be. And a good idea we we would look at something that is a little bit more worthy still, short enough but so that it can also be and and parsed by by machine on the bottom. You see the respective attestation statements. For instance, you see the one

1113
03:20:45.390 --> 03:20:49.020
Werner Staub: the one about. And

1114
03:20:49.150 --> 03:21:03.650

Werner Staub: this year, you know. So basically, it just has these values in the Dns. What we lack here because we didn't want to go, you know, and start the project without the agreement of the sports federations before we didn't put the

1115
03:21:04.020 --> 03:21:22.179
Werner Staub: the claim statement. So if you want to see a claim statement. We put one, for instance, in the case of of our own, you know, cooney.org domain name. So you see, we created an attribute leaf public ids.coy.org and

1116
03:21:22.948 --> 03:21:46.949
Werner Staub: underscore public ids chronicle board and underscore references dotcorny.org and they just point to the res respective resource. You know the machine that's supposed to understand this will know where to look in order to to to check. If this is this is a demo I focus here on the one that bbus be using for sports. So this might actually, if it was a sport domain.

1117
03:21:46.950 --> 03:22:03.294
Werner Staub: It might probably point to either sport record itself, or you might probably use specific dedicated domains, such as id dot sport, and the to do this when I say we I know put my dot sport and head on hat on.

1118
03:22:03.710 --> 03:22:14.613
Werner Staub: because, you know, we try to do this as a, as a, as a, as a project that will support the the sport community from that from that side. Side.

1119
03:22:15.590 --> 03:22:20.484
Werner Staub: By the way, it's just, you know, this is a an illustration, you know, for how

1120
03:22:21.420 --> 03:22:33.989
Werner Staub: available data looks like what you see here is the domain name in one of those frauds that are displayed over Youtube, and for which Google has said that they have verified the Advertiser.

1121
03:22:34.980 --> 03:23:01.259
Werner Staub: So this is, you know. No, here's in Bulgaria, and they're the advertis supposed to be in in in Poland, and of course it says Gdpr. Masked, and so on, and it is falling into the mainland this around there. For 2 months, you know. Almost 2 months, and there's nothing happening to it, because it's it's really hard to. I see them because most of the people who should see them. They don't see them.

1122
03:23:02.470 --> 03:23:21.350
Werner Staub: I can go to look at a couple of of other cases, you know. See, you know, we did this just with on the basis of what we call a report statement for somebody who should, you know, do something about their domain. They're doing some of it, but not all of it. Of course they should.

1123
03:23:21.350 --> 03:23:35.129
Werner Staub: This is outside of the sport community. But those are quite relevant because it's a payment. It's a payment side. What is actually, you know, in this case worth mentioning is that they have

1124
03:23:35.270 --> 03:23:37.219
Werner Staub: a legal entity identifier

1125
03:23:37.530 --> 03:23:40.569
Werner Staub: and the legal identified identifier as

1126
03:23:40.640 --> 03:23:42.550
Werner Staub: and a

1127
03:23:42.790 --> 03:23:44.280
Werner Staub: a

1128
03:23:45.980 --> 03:23:59.069

Werner Staub: a link to the domain name. But it's not visible if you look at under no, under this, under this here you would have to go to Google Lei, and also sorry to Bloomberg Lei.

1129
03:23:59.330 --> 03:24:02.859
Werner Staub: and search this as a Bloomberg Lei.

1130
03:24:03.020 --> 03:24:05.879
Werner Staub: and then it would show that

1131
03:24:05.970 --> 03:24:24.469
Werner Staub: the domain name here is wise.com. That's part of the data model of the Bloomberg, but is not part of the data model, or yet of life itself. So life is considering adding such a thing to their data model, and then, of course, would also, you know, support, look up by the Dns.

1132
03:24:24.820 --> 03:24:42.810
Werner Staub: And what else do we have, you know, and I might just give a couple of shocking examples here. In terms of lack of information to the public. We have our registry for.org pir. That apparently is not supposed to be known to the public.

1133
03:24:42.910 --> 03:25:07.999
Werner Staub: and says, is hidden by domain by proxy. The same thing is isopad or domain by proxy or Internet society.org domain by by proxy. So let's say, this is just, you know, an indication of where you know where things are going. And so, as we work on, you know, we're trying to work hard on our app, and then we, you know, most likely. See that our back is mostly our app is mostly being evaded.

1134
03:25:08.020 --> 03:25:18.280
Werner Staub: And what whatever effort we're making seems to be increasingly an exercise in futility, because there's no, there's no data going to be displayed in the in. In in the 1st place.

1135
03:25:20.655 --> 03:25:21.620

Werner Staub: a.

1136
03:25:21.800 --> 03:25:44.999
Werner Staub: As we work. You know, Internet governance. We might actually also think about how we would attest to Internet governance organizations. This was one of the things that just. You know we ran that for for Icann we probably might think. You know, you know, sports does something hopefully. Other sectors will come up with. You know them their own. So we could actually, you know, make sure that

1137
03:25:45.070 --> 03:25:50.879
Werner Staub: you know the habit of providing attestations specific for legal entities

1138
03:25:51.080 --> 03:26:03.230
Werner Staub: are actually proposing resources that involve quite a bit of a risk for the end user they should actually attest to their credibility and to their standing.

1139
03:26:03.290 --> 03:26:06.469
Werner Staub: That's all I have, you know, if there's any questions, and I'm happy to answer.

1140
03:26:08.110 --> 03:26:31.249
Hadia Elminiawi: Thank you so much. Warner. For this presentation. And we have a question from Patrick. He says. Suggestion subject. Verb object seems very similar to, if not the same as Rdf. Not possible to reuse pieces of it instead of redefining everything. Also, I don't think this should be in text records at all.

1141
03:26:33.940 --> 03:26:36.800
Werner Staub: Yeah, I actually, I I've

1142
03:26:37.170 --> 03:26:47.709

Werner Staub: spend quite a time to Simon, thinking that was is probably the good point that text records could have issues. You know. I saw that, for instance, you know some some parties for

1143
03:26:47.900 --> 03:26:54.679
Werner Staub: for text records. They have Wildcard text records. You know, that actually defeat some of the, you know.

1144
03:26:54.840 --> 03:26:59.352
Werner Staub: but the ease of use, or maybe not the purpose, but the ease of use, of retrieving a sub

1145
03:26:59.780 --> 03:27:01.470
Werner Staub: an attribute leave.

1146
03:27:01.570 --> 03:27:02.550
Werner Staub: and that.

1147
03:27:02.790 --> 03:27:15.689
Werner Staub: But the I'm not quite sure. If a text record is, however, the wrong you know the wrong approach. I think it may be that the text record will be the best solution.

1148
03:27:15.990 --> 03:27:29.790
Werner Staub: The the current project will probably most probably use text records, at least for the attestation part. We might still, you know, open the the the debate to you know, the creation of a new attestation record.

1149
03:27:29.850 --> 03:27:40.229
Werner Staub: It quickly runs into problems. I mean, we say, yes, it's an attestation record, you know. Does that mean? It's, you know it has some some meaning, just because it is an attestation record.

1150
03:27:40.250 --> 03:27:47.409

Werner Staub: And I think it's it's important to remember that the credibility must always depend

1151
03:27:48.240 --> 03:27:58.310
Werner Staub: the credibility of the issue of the statement. So it couldn't be. Is it just because there is such a thing, you know, then it would be, and it would have to be believed.

1152
03:27:58.370 --> 03:28:08.860
Werner Staub: It is, you know, for the party that uses it to use a chain of reasonable inferences, and to be sure that they can, they can use that.

1153
03:28:09.790 --> 03:28:22.949
Werner Staub: It is also probably useful as a text record, because to attest to something must be reasonably precise in terms. What are you really attesting to? So there's a methodology behind it.

1154
03:28:23.020 --> 03:28:28.930
Werner Staub: And just say, there's a standardized record as we do this in Spf or in deacon or in Dane.

1155
03:28:29.395 --> 03:28:46.829
Werner Staub: That's fine. If you get 2 big problems. First, st of all, these records are cryptic. Secondly, there is specific. So if it's not exactly that use case you cannot use them. But let's say we should. We should be able to

1156
03:28:47.189 --> 03:29:11.260
Werner Staub: create, you know, and favor the creation of an ecosystem where attestations are being used that are outside of the frame of the browser. So it must not be inside of what the browser presents, it must be outside for name. The browser, or the app can verify it independently, and not be dependent on whatever logo has been copied by the pirates who present the website.

1157
03:29:13.795 --> 03:29:21.109

Hadia Elminiawi: Thank you, Werner. And then, there is another question that says, How will this handle a a registration change.

1158
03:29:23.690 --> 03:29:33.999
Werner Staub: So the essence is that you know a a domain might be held, you know, by a certain party. So and then that party might give up on the on that domain.

1159
03:29:34.140 --> 03:29:37.949
Werner Staub: So you might have credit Suisse, you know the bank.

1160
03:29:38.621 --> 03:29:48.009
Werner Staub: And credit Suisse. The bank has been purchased by Ubs, and eventually credit. Suisse will no longer be

1161
03:29:48.535 --> 03:30:00.430
Werner Staub: trading under. You know the its own name, so it would be trading under under ubs. Now, if you look at that, you know, Zoom, I don't think that, you know, for anything that is the typical.

1162
03:30:00.530 --> 03:30:18.439
Werner Staub: the typical object of malicious impersonation. There would that would be highly frequent, and, you know, keeping a domain name alive, and then removing the attestation to it, you know, is is probably not so. Not so hard. In the.

1163
03:30:18.440 --> 03:30:39.629
Werner Staub: In the case of other forms of attestation everybody knows, and where we can only wonder why we do not have to mean domain names when they have existed in finance for 100 years. And the ratings, you know, they're updated on their regular basis, and doesn't mean that if in a if an organization had a triple, a rating, you know, 10 years ago, they just still have one now.

1164
03:30:39.630 --> 03:30:58.349

Werner Staub: or even it was just 3 months ago. That doesn't mean they have it now. So the checking of this is actually quite valid, you know, it's actually quite useful, and you know, just takes a couple of milliseconds, and we don't have to retrieve the revocation list, you know, just as soon as the at the station is removed.

1165
03:30:58.580 --> 03:31:09.559
Werner Staub: it's gone. We might even actually come up with at the station to say, this is now being withdrawn. It is no longer is no longer the the being attested to.

1166
03:31:12.880 --> 03:31:33.520
Hadia Elminiawi: Thank you. Werner and I I don't see any any more hands up and nothing in the chat. So I I guess we can now move to Gotham accuweate from Stanford University, and he will be talking about best practices for deletion in Epp

1167
03:31:36.320 --> 03:31:38.579
Hadia Elminiawi: Gautam, the floor is yours.

1168
03:31:38.960 --> 03:31:45.530
Gautam Akiwate: Thank you. How do you? Let me? Okay, I'm assuming folks can see my screen.

1169
03:31:47.980 --> 03:31:50.849
Hadia Elminiawi: We? We see your screen perfect. Thank you.

1170
03:31:51.160 --> 03:32:01.669
Gautam Akiwate: Awesome. So thank you. Hi, my name is Gotham Akiwa, and I'm a researcher at Stanford University, and today I'm going to talk about

1171
03:32:02.540 --> 03:32:06.410
Gautam Akiwate: to talk about best practices and deletion of upp.

1172

03:32:06.550 --> 03:32:17.580
Gautam Akiwate: and as the subtitles suggest, the reason we are interested in looking at deletion of Epps is because of risks that arise as a result of the Cpp name management.

1173
03:32:18.580 --> 03:32:35.340
Gautam Akiwate: And even though I am going to be the one talking here a lot of this presentation is based on an Internet draft that is making its way through the Digx working group, and Scott and Bill have both been instrumental in making this Internet draft happen.

1174
03:32:35.720 --> 03:32:58.580
Gautam Akiwate: Okay, so let's talk about why we care about deletions in Epp, and you must be wondering, like, it seems like an oddly specific topic, like deletions in Epp is like oddly specific. And then and let me set up some context as to why we are interested in in Epp deletions, specifically.

1175
03:32:58.580 --> 03:33:21.699
Gautam Akiwate: And the reason we started looking into this we started investigating was that in course of some of our research, when we were looking for domain hijacks, we stumbled across this really odd mystery, and this was like a whodunit mystery where we saw a domain. And in this case, like an official county domain for a domain in Georgia

1176
03:33:21.700 --> 03:33:32.200
Gautam Akiwate: County, in Georgia, where the name server changed from Ns. 2. Internet emccom to Nsu Internet random characters.

1177
03:33:32.670 --> 03:33:34.680
Gautam Akiwate: Now, what was interesting about

1178
03:33:34.930 --> 03:33:38.519
Gautam Akiwate: Internet Dmc random characters. So this was that

1179
03:33:38.930 --> 03:33:58.100

Gautam Akiwate: it was not registered. So a thread actor could reasonably just go in register Internet Emc at random characters.biz, and be the authoritative name server for white county.net. So the share of queries that come to Nsu at Internet Emc at random characters.biz.

1180
03:33:58.290 --> 03:34:12.999
Gautam Akiwate: they could control where the where it sort of. And we were doing this research in 2,020 and county domains also on election infrastructure. So all of this be felt a little bit frightening.

1181
03:34:13.020 --> 03:34:24.870
Gautam Akiwate: But this was not the only domain that was that that was that showed similar behavior. What we found was that nearly half a million domains

1182
03:34:25.342 --> 03:34:36.609
Gautam Akiwate: we're exposed over to the last 10 years, and all of them had similar patterns. And what we realized was that these large numbers indicated a systemic risk.

1183
03:34:36.980 --> 03:34:48.780
Gautam Akiwate: And given this systemic issue, we sort of went back to a drawing board and figured out like, where in this pipeline in the Dns configuration, pipeline, could this arise?

1184
03:34:48.870 --> 03:35:16.219
Gautam Akiwate: And, roughly speaking, it seemed like there were 2 potential places like either. The registrant itself was making some changes that were being propagated. But given this, the the systemic nature, and also the large numbers and the pattern that we saw. We realized that it had to be an an outcome of Epp, and how registrars were interacting with the Epp with the protocol.

1185
03:35:16.570 --> 03:35:39.799
Gautam Akiwate: Okay, so let's work through what? Exactly in Epp, what are exactly this in Epp like that manifests itself here. Okay, so let's say we have 2 domains, Foodcom and Barcom, and Foodcom is registered by registrar A.

It's managed, sponsored by registrar A, and Bar Com is Sponsored by Registrar B.

1186
03:35:40.590 --> 03:35:53.500
Gautam Akiwate: Now let's introduce some of the Epp terminology. So food.com is a domain object, and it has to subordinate host objects. Ns, one dot food com, and then a student food com

1187
03:35:53.540 --> 03:36:01.760
Gautam Akiwate: bar.com, which is a domain object, on the other hand, has a single subordinate host. Object Ns. one.bar.com.

1188
03:36:01.910 --> 03:36:26.689
Gautam Akiwate: Now, the interesting thing about bar.com is that it uses Ns one.bar.com as a name server, which is its own subordinate host object, but also Ns. 2.4.com, which is managed by a completely different registrar. So bar.com uses a host object that is managed by a different register that is, belongs to a different domain, and this is perfectly fine. This is a 3rd party dependency.

1189
03:36:26.690 --> 03:36:33.140
Gautam Akiwate: and this is exactly how we expect bens to work, and all of this works fine

1190
03:36:33.570 --> 03:36:36.180
Gautam Akiwate: till food.com expires.

1191
03:36:36.300 --> 03:36:38.969
Gautam Akiwate: Now when food.com expires.

1192
03:36:39.381 --> 03:36:49.670
Gautam Akiwate: the Epp. Rfc. 5, 7, 3. One tells us that a domain object should not be deleted if subordinate host objects are associated with the domain. Object

1193

03:36:50.600 --> 03:37:04.090
Gautam Akiwate: that makes sense. Given this guidance, we need to go through and delete the host objects. So we go in. We delete Ns. one.2.com. Not a problem. But when we go to delete Ns 2.4.com.

1194
03:37:04.150 --> 03:37:09.059
Gautam Akiwate: Epp does not allow it. Allow this operation to go ahead.

1195
03:37:09.270 --> 03:37:25.440
Gautam Akiwate: and the reason that it does not allow it to go ahead is because of guidance and deletion. In Rfc. 5, 7, 3, 2. Which says that a host object should not be deleted if the host object is associated with any other object, and in this case

1196
03:37:25.980 --> 03:37:29.350
Gautam Akiwate: nistew.food.com is associated with bar.com.

1197
03:37:29.790 --> 03:37:49.699
Gautam Akiwate: and if the register now wants to delete it, the host object should not be deleted until the existing association has been broken. So the register now needs to find a way to break this association between bar.com and Nsu dot foodcom.

1198
03:37:50.090 --> 03:38:13.650
Gautam Akiwate: And what registers have sort of come to find is that renaming have sort of landed on a set of operational practices which use renaming to break this association between food.com and NS. 2.4.com so concretely. What they do is that they rename Ns. 2.4.com to NS. 2 dot 4, say random characters dot this.

1199
03:38:13.650 --> 03:38:24.339
Gautam Akiwate: And this just basically renames the host object to an external top level domain, which now means that it is no longer a subordinate host object of who dot.

1200
03:38:25.090 --> 03:38:32.189

Gautam Akiwate: which means that food.com no longer has any subordinate host objects, and can be deleted by the register.

1201
03:38:32.540 --> 03:38:40.560
Gautam Akiwate: and at the end, what we're left with is with a sacrificial name, server, what we call a sacrificial name server.

1202
03:38:40.580 --> 03:38:47.860
Gautam Akiwate: So bar.com started this journey with 2 name servers and a swan.bar.com, and then a student@food.com.

1203
03:38:48.490 --> 03:38:53.750
Gautam Akiwate: but ends it with NS. 2 dot 4 random characters dot base.

1204
03:38:53.950 --> 03:39:02.049
Gautam Akiwate: and this is happening without bar.com. Ever realizing that one of its name server that it depended on was renamed underneath it.

1205
03:39:02.640 --> 03:39:05.259
Gautam Akiwate: Okay, so this

1206
03:39:05.614 --> 03:39:12.730
Gautam Akiwate: a lot of this. What, what a lot of what we were talking about was with the assumption that we are working in a single top level domain.

1207
03:39:13.260 --> 03:39:39.070
Gautam Akiwate: But from an example like there were a bunch of top level domains that were involved. That was.net.com. And we still haven't sort of talked about how this affect spans, how this renaming spans multiple domains. So let's sort of expand the scope a little bit and try and understand how the renaming affects different top level domains. So as it turns out, the renaming affects

1208
03:39:39.070 --> 03:40:04.950

Gautam Akiwate: all of the top level domains in a given Epp repository. So now, in our left in our very sign, Epp Repository, which used to manage.com as well. Foodcom and.gov are part of the same Epp repository. So they share. And let's say, in an case this.gov domain uses, and it's 2.4.com. Then they are sharing the same host object.

1209
03:40:05.080 --> 03:40:15.609
Gautam Akiwate: On the other hand, the boss.org domain, the failures the Epp repository uses NS. 2.4.com

1210
03:40:16.403 --> 03:40:30.279
Gautam Akiwate: which is like a host object that is separate. So the there are 2 host objects, and the the sharing only spans a single Epp repository. So now, when foodcoms expires.

1211
03:40:30.733 --> 03:40:49.289
Gautam Akiwate: We sort of run into the same issue, and then, when the register, a sort of Renames sec the nsd.food.com. We end up with a sacrificial name server in the Verizon Epp repository, Soc. Gov. Ends up with a sacrificial name server, while, on the other hand, pass.org

1212
03:40:49.390 --> 03:40:53.560
Gautam Akiwate: ends up with a link delegation which is nsu.food.com.

1213
03:40:53.620 --> 03:40:59.170
Gautam Akiwate: and that in essence is the difference between sacrificial name service for Sicily and delegations.

1214
03:40:59.574 --> 03:41:15.155
Gautam Akiwate: We expect sacrificial name service to be lame, but there are cases in which it might not be lame, delegated, and I know there is some conversation about like we don't use the terms name delegated like. There are other things, but this is how we are like

1215
03:41:15.500 --> 03:41:22.169

Gautam Akiwate: that aside, this is how we sort of understand the difference between sacrificial name, service, and name delegation. Okay.

1216
03:41:22.550 --> 03:41:27.670
Gautam Akiwate: so given that we now understand the importance of pollution.

1217
03:41:28.300 --> 03:41:51.470
Gautam Akiwate: How do we? What are the different practices. And how do we do it? Right? Okay? So there are 2 broad categories of how we can approach deletion and and like in thinking about best practice as well. The 1st is just renaming, but doing, renaming better, and the second is just allowing deletion. So Rfc. Guideline says.

1218
03:41:51.880 --> 03:42:05.910
Gautam Akiwate: should not delete. But what happens if we just allow deletion. So let's let's sort of work through those 2 categories of practices. But let's start out with looking at renaming practices.

1219
03:42:06.230 --> 03:42:28.750
Gautam Akiwate: Okay? So the renaming practices, the 1st one which which is what currently happens, which is the renaming to external, presumed non-existent hosts. So in this case, as we saw, like Ns one.4.com. It's renamed to Ns one dot 4 random directors dot this, and this in essence is to

1220
03:42:29.374 --> 03:42:34.829
Gautam Akiwate: break the existing association between the domain object and the host object.

1221
03:42:35.580 --> 03:42:50.099
Gautam Akiwate: Now, assuming that we don't want to have this domain be registrable, we could use a special use top level domain. So instead of renaming it to dot base, we could rename it to something like dot invalid.

1222
03:42:50.510 --> 03:43:07.070

Gautam Akiwate: And if we want it to be even more strategic, which sort of indicate what is the the nature of this domain? We could use a special use domain, something like sacrificial invalid, so that the when the registrar is renaming the

1223
03:43:07.200 --> 03:43:13.630
Gautam Akiwate: a host object, it could use sacrificial and invalid as its target top level domain.

1224
03:43:14.020 --> 03:43:33.789
Gautam Akiwate: I know that some registrators are also using as 1, 1, 2 dot, one as the renaming as it's renaming target. And again, as 1, 1, 2. cannot be registered. And that's why it was thought desirable. Except like, if you go read that Internet drop, we sort of go through a bunch of reasons as to why

1225
03:43:34.171 --> 03:43:42.249
Gautam Akiwate: why we shouldn't do as 1, 1, 2.com. And finally, we have this managed sacrificial name, service space. So instead of

1226
03:43:42.280 --> 03:43:47.510
Gautam Akiwate: and and this is also something that we see quite a lot of where registrars

1227
03:43:48.407 --> 03:43:58.190
Gautam Akiwate: basically register a domain name which they then use as the renaming target for all of the renamings that they are sort of doing.

1228
03:43:58.300 --> 03:44:06.939
Gautam Akiwate: And what this means is that in this one dot foodcom would get mapped to a domain under registrar dot example.

1229
03:44:07.210 --> 03:44:35.799
Gautam Akiwate: The upside of it is that the register, like the domain, is not registrable, so folks cannot hijack it, and Ted actors cannot hijack it. But a downside of this is, if the registrar displaces an undivision on the register, where, if they sort of go out of business or like change operational practices,

then they have to keep this registrar domain registered at all points of time, and if any point in the future like they let they let

1230
03:44:36.186 --> 03:44:48.303
Gautam Akiwate: let the registration elapse, then a thread actor can come in, register the domain and be the broader lot of like thousands of domains, which sort of in increases the the scope of vulnerability.

1231
03:44:49.010 --> 03:45:00.240
Gautam Akiwate: So in order to avoid that, one could imagine that we could also have community manage sacrificial name servers. So instead of like sort of having a per registrar

1232
03:45:00.707 --> 03:45:20.209
Gautam Akiwate: sacrificial name, silver name, we could have, like a a sacrificial dot example that is being met operated by somebody, that is, let's say, assigned to by act so like it would be a community. Manage sacrificial name server that way. We sort of reduce the discopet. It's registration elapsing.

1233
03:45:20.600 --> 03:45:45.199
Gautam Akiwate: Okay? So out of all of these, I think we think that most of them are reasonable except for as 1, 1, 2 dot and the external presume non existing host. So I think given if you folks have like sort of looking at, we name practices. We have a detailed breakdown of like the detriments and the benefits of each of these approaches

1234
03:45:45.200 --> 03:45:59.699
Gautam Akiwate: in the in the Internet draft. But, roughly speaking, like most of these, should work fine, and in the summary we'll sort of talk about what we think of the best practices, but, like any of these approaches seem reasonable

1235
03:46:00.190 --> 03:46:10.999
Gautam Akiwate: as long as you don't do external or S 1, 1, 2 dot. Okay? So the second category of approaches to to order.

1236
03:46:11.010 --> 03:46:15.709
Gautam Akiwate: Deletion is to just allow post object deletion, and concretely

1237
03:46:15.990 --> 03:46:45.370
Gautam Akiwate: it to allow nsu.food.com to be deleted, even though it is being us. It. It is associated with another domain object. In this case, bar.com. So even though nsu.food.com is associated with bar.com we are going to like. Allow it to be deleted, and what that will end up looking like is bar.com will have a single name server, Ns. one.bar.com

1238
03:46:45.967 --> 03:47:05.809
Gautam Akiwate: and this scenario was exactly what the guidance was trying to avoid. The guidance was trying to ensure that power.com always had 2 name servers, but if you think about it, in our previous state of affairs the second name server was essentially a rename, safe name server that wasn't really useful.

1239
03:47:05.870 --> 03:47:22.680
Gautam Akiwate: And we feel like this deletion this represents like, even though it's single name, server. It represents the true state of affairs, and is something that the registrant can notice is something is a mess, and like will take remediation action sooner.

1240
03:47:23.487 --> 03:47:50.639
Gautam Akiwate: So, assuming that you allow for, like a. The registry allows for deletion. Then there are a bunch of different flavors that can be done in the deletion where register can explicitly request deletion, and in order to make sure that there are no accidental deletions we could delete with like a restored capability, where if there is an accidental deletion, then we can revert the deletion.

1241
03:47:51.350 --> 03:48:20.259
Gautam Akiwate: And if you're feeling really fancy we could also do deletion with notification which would allow which in which registries could notify other registries and registrars which feels a daily complicated, but in theory they could notify other registrars and registries of deletions that deletion

requests that they have received and successfully executed, and this will allow us to sort of deal with lame delegations. As as we thought of them previously.

1242
03:48:20.480 --> 03:48:21.510
Gautam Akiwate: so

1243
03:48:21.720 --> 03:48:40.810
Gautam Akiwate: in summary like. There are 2 categories renaming, and allow deletion for practices, and in general, like right now, the best current practice seems to be manage sacrificial name service, and specifically where registrar sort of manage their own sacrificial name service.

1244
03:48:41.420 --> 03:48:58.970
Gautam Akiwate: But as we had discussed this doesn't feel like a sustainable long term solutions because registers, and what would like to change operational practices all the time, and like they, we wouldn't want Regis to sort of keep on top of having to register this one domain

1245
03:48:59.374 --> 03:49:25.569
Gautam Akiwate: for years and years together. So we propose, like the 2 best practices would be for just to allow deletion. And I think allowing deletion will simplify a lot of this workflow. That said, we know that not all registries allow for deletion but this would require some change. So there is, some effort that needs to go in to actually allow for deletion. But assuming that that sort of

1246
03:49:25.957 --> 03:49:45.349
Gautam Akiwate: is something that can happen then allow deletion is probably the best bet, but in case that cannot happen in terms of renaming the use of special use, domains, would be the best practice, even though we don't really have a suggestion for what? Exactly to use there.

1247
03:49:46.142 --> 03:49:55.189
Gautam Akiwate: But with that I'm happy to take any questions, and also answer any questions that are.

1248
03:49:55.950 --> 03:49:57.479
Gautam Akiwate: and keep it short and sweet.

1249
03:49:57.480 --> 03:50:06.689
Hadia Elminiawi: Thank you. Yeah, thank you so much. Gotham, for this explanation. And for the presentation it was very clear. And

1250
03:50:06.920 --> 03:50:19.110
Hadia Elminiawi: so actually, I don't see any questions on the QA. Pod. I I also don't see any any raised hands.

1251
03:50:20.041 --> 03:50:27.988
Hadia Elminiawi: So I guess we currently don't have any questions for you. I guess you were so clear and

1252
03:50:28.760 --> 03:50:45.609
Hadia Elminiawi: we have 8 min left until the end of this workshop. We now are at the open discussion part, and we did take all the questions during the presentations and the panel discussion.

1253
03:50:46.510 --> 03:51:15.350
Hadia Elminiawi: So before we start the open discussion, I would like to remind you that to help us better prepare future arose. Please respond to a 5 min survey for a row 13, the link is available in the chat and on our website, or it will be available now in the chat. And also it's available on our website.

1254
03:51:16.902 --> 03:51:40.259
Hadia Elminiawi: So a, again, we open the floor. Now for open discussion. This is an opportunity to ask questions and and share your thoughts with our panelists. Please. Again use the Q&A pod as you have been using throughout the workshop, or raise your hand. so, Edward, please go ahead.

1255
03:51:42.400 --> 03:51:46.469

Edward Lewis: Oh, it's it's it's not me! It's there is a question in the QA. From Patrick.

1256
03:51:46.470 --> 03:51:56.050
Hadia Elminiawi: Oh, oh, okay, sorry yeah. I see it now. Thank you. So Patrick is saying or Patrick, would you like to? Take the mic.

1257
03:52:05.090 --> 03:52:07.690
Steve Conte - ICANN Org: Patrick, I enabled phone. There we go. Thank you.

1258
03:52:07.950 --> 03:52:09.240
Patrick Mevzek: Do do you hear me?

1259
03:52:10.830 --> 03:52:11.710
Hadia Elminiawi: A week.

1260
03:52:13.260 --> 03:52:14.550
Patrick Mevzek: Do you? Do you hear me?

1261
03:52:15.440 --> 03:52:18.950
Hadia Elminiawi: We hear you loud and clear. Clear! Patrick, go ahead, please.

1262
03:52:18.950 --> 03:52:22.779
Patrick Mevzek: Okay? Great. So, yeah, my question was on the last presentation. If

1263
03:52:22.960 --> 03:52:31.480
Patrick Mevzek: the subject of considering, because Epp has a dual model for managing name server. So was it considered

1264
03:52:31.590 --> 03:52:57.289

Patrick Mevzek: to maybe leverage that more on to allow some kind of mixing setup where us objects that need to be needs to be deleted would be kind of under as attributes or not anymore as objects. And then that would like that would break the association on Reserve. The deletion problem. So just a question. If that was considered or not.

1265
03:52:57.530 --> 03:53:13.179
Gautam Akiwate: So I don't think we ever considered a mixed host. Object host, attribute model. I think when we were sort of looking into this issue when we're talking to different registries. I think our understanding was that the host attribute model is not as widely used.

1266
03:53:13.430 --> 03:53:22.120
Gautam Akiwate: and it's primarily the host object model that gets used. And I'm not sure if any of the registries, like actively considered

1267
03:53:22.140 --> 03:53:29.210
Gautam Akiwate: shifting to like a host, attribute model just for this, or adopting, like a mixed use model.

1268
03:53:29.675 --> 03:53:40.320
Gautam Akiwate: So I think, generally speaking, what seems to have happened? It's 1 or the other, but not both. Yeah, I think that's accurate. And

1269
03:53:40.987 --> 03:54:05.629
Gautam Akiwate: I think, given given the sense that I had talking to registries like the host object model is the more dominant, like by far the most dominant I think I know of. Maybe one top level domain like maybe others. A CCTV like dotcl uses the host attribute model. I'm sure there are others, but predominantly. It's the host object model, that is really dominant.

1270
03:54:06.970 --> 03:54:30.669
Patrick Mevzek: Yeah, I I agree it's dominant. But it's exactly the one creating the problems in the 1st place. So that's that's my. That's why I asked that. Because if you are using us attributes on big CCTV, these are

using us attributes. you don't have the exact program you mentioned. So that's why I was curious. If it was consider, obviously creating lots of other problems. But just curious.

1271
03:54:30.910 --> 03:54:50.330
Gautam Akiwate: Yeah, it feels like a big lift. And i i i don't know if registry is like, honestly, con like thought of moving towards a host model. But you're right in that. This is actually only a problem in the host. Object model and not a host attribute model. So you're we're spot on there.

1272
03:54:54.770 --> 03:54:55.160
Patrick Mevzek: Thank you.

1273
03:54:55.160 --> 03:54:55.820
Hadia Elminiawi: And you.

1274
03:54:57.130 --> 03:55:09.309
Hadia Elminiawi: Thank you. thank you, Jim. And so there! Sorry. Thank you, Gatam, and there is a comment from Jim. He says, I believe it's 1 or the other, but not both.

1275
03:55:10.500 --> 03:55:11.230
Hadia Elminiawi: And

1276
03:55:14.150 --> 03:55:19.300
Hadia Elminiawi: okay, so no more questions

1277
03:55:19.879 --> 03:55:36.669
Hadia Elminiawi: I guess we can now move to the closing slide. We are we have only 3 min left until the end of this workshop. I remind you to please respond to row 13 survey

1278
03:55:36.860 --> 03:55:40.599
Hadia Elminiawi: and if we can have the closing. Yes.

1279
03:55:40.750 --> 03:55:49.869
nicoleta munteanu: Hi! Apologies. This is Nicole. If Alex is still online I was wondering if he could answer Jody's question in the QA. Pod.

1280
03:55:51.840 --> 03:55:52.893
Alexander Mayrhofer: Yes, sure.

1281
03:55:53.630 --> 03:55:54.639
Alexander Mayrhofer: there it is.

1282
03:55:55.350 --> 03:55:56.780
Alexander Mayrhofer: Jody.

1283
03:55:58.950 --> 03:56:02.390
Alexander Mayrhofer: That is the will. The register be able to verify the information

1284
03:56:04.150 --> 03:56:06.830
Alexander Mayrhofer: correctly without verifying in an identity.

1285
03:56:11.470 --> 03:56:17.640
Alexander Mayrhofer: I honestly sorry, Jody, can you clarify? Because I don't understand the question? I'm afraid.

1286
03:56:17.970 --> 03:56:19.179
Jody Kolker: Sure if I like.

1287
03:56:19.180 --> 03:56:20.700
Alexander Mayrhofer: Sure! Hey! Jody! Hi!

1288
03:56:20.700 --> 03:56:28.100
Jody Kolker: Hey, hey, Alex? Oh, thanks for the presentation 1st of all. But but what I'm curious is, will the registrar be allowed

1289
03:56:28.180 --> 03:56:35.990
Jody Kolker: to verify this information without having to go to another entity. For instance, if it's a passport of bank. Okay, thank you. That's all.

1290
03:56:35.990 --> 03:56:47.200
Alexander Mayrhofer: Yes, this is just for the case that they actually want to like outsource this to another entity, but they can perfectly say success and entity, or agent, as we call it, would be like the register name itself.

1291
03:56:47.290 --> 03:56:48.299
Alexander Mayrhofer: That's what I have.

1292
03:56:48.450 --> 03:56:49.060
Jody Kolker: Alright!

1293
03:56:49.060 --> 03:57:02.629
Alexander Mayrhofer: We haven't created any any structure for that field yet. We might. But then, as you know, we might get into the problem locking rate to registry of entities. And so we said, Ok, let's do it a clear text field. And if our

1294
03:57:02.640 --> 03:57:14.019
Alexander Mayrhofer: I don't know, legal department goes to the register and tries to audit them, and says, Hey, you told us that this entity actually did verification, and that the referral number give us the documents so as easy as that.

1295
03:57:14.300 --> 03:57:15.570
Jody Kolker: Excellent. Thank you.

1296
03:57:16.240 --> 03:57:17.959
Alexander Mayrhofer: In my thought. Thank you.

1297

03:57:19.490 --> 03:57:25.049
Hadia Elminiawi: Thank you. Jody and thank you. Alexander, for the reply.

1298
03:57:25.180 --> 03:57:36.309
Hadia Elminiawi: and I I guess, Alexander, you did say at some point that you do not actually ask registrars whether they verify the information or not, or how to do it. Is that true.

1299
03:57:37.380 --> 03:57:38.679
Alexander Mayrhofer: And so

1300
03:57:38.690 --> 03:57:46.490
Alexander Mayrhofer: the second part of your statement is true. The 1st one is not true. So we definitely ask registrars to verify the information. So

1301
03:57:46.510 --> 03:57:54.119
Alexander Mayrhofer: if they say verification success, and we expect them to have verified information in their in their contact objects.

1302
03:57:54.290 --> 03:57:55.030
Alexander Mayrhofer: But

1303
03:57:56.250 --> 03:58:09.300
Alexander Mayrhofer: yeah, so we don't ask him to provide the actual proof of verification to the registry, because we believe it might also get very complicated. We don't wanna sit on a pile of passport copies quite frankly.

1304
03:58:11.140 --> 03:58:11.629
Alexander Mayrhofer: Thank you.

1305
03:58:11.630 --> 03:58:12.140
Hadia Elminiawi: I don't.

1306
03:58:12.140 --> 03:58:13.210

Alexander Mayrhofer: Yeah. Wonderful. February.

1307
03:58:13.210 --> 03:58:13.570
Hadia Elminiawi: Ok. Chef.

1308
03:58:13.570 --> 03:58:22.120
Alexander Mayrhofer: Sorry if I have 20 more seconds. Registrants have different business models, some of the largest registrars under audio. These are actually telco providers.

1309
03:58:22.360 --> 03:58:34.330
Alexander Mayrhofer: and, as I said, they might have like a business relation with the customers in 25 years, because they also provided the Dsl. Account. So it feels awkward at that point in time to request a passport copy or something.

1310
03:58:37.600 --> 03:58:40.320
Hadia Elminiawi: Thank you so much for the clarification. This

1311
03:58:40.710 --> 03:58:47.779
Hadia Elminiawi: idea again for the record. And Nicoletta, can we now have the closing slide?

1312
03:58:53.460 --> 03:59:06.429
Hadia Elminiawi: Thank you. So we invite interested parties to let us know by email of their willingness to sponsor future workshops and become members of the program committee that coordinates show events

1313
03:59:07.052 --> 03:59:16.617
Hadia Elminiawi: again. Please remember to respond to the survey. And finally, I would like to.

1314
03:59:17.754 --> 03:59:27.870
Hadia Elminiawi: Thank our sponsors very sign, and I can also a big thank you to our speakers and to all of you for taking part in row. 13.

1315
03:59:27.960 --> 03:59:43.879
Hadia Elminiawi: Oh, I stop here. Thank you all for allowing me to moderate this workshop, and I am not sure whether to pass. Pass the mic to Steve or Nicoletta. But the floor is yours.

1316
03:59:47.860 --> 03:59:56.760
nicoleta munteanu: Thank you, Hadya. Thank you for accepting to moderate the session. Thank you. Everyone for joining us today. See you at the next row.

1317
04:00:00.730 --> 04:00:02.660
Alexander Mayrhofer: Thank you. Everyone. Bye.