Di **[00:00:13]**: We are so glad to welcome Tony Lucich from Orange County, California. Tony, may we ask you to introduce yourself and tell us how you fit into the identity provision and technical privacy enforcement world?

Tony: Certainly. I'm welcomed to be here. Tony Lucich, I'm the Information Security Officer for the County of Orange. In California, the County of Orange does not include the Superior Court system, so I'm the liaison from the county side. We have [Superior Court Chief Technology Officer] Snorri [Ogata], who is the liaison from the court side, so I'm the glue in that metric. Relative to this activity, I'm the sponsor and coordinator for our identity solution. We call it O-C-I-D, for Orange County Identity.

[00:01:01]

OCID is now being used to connect a variety of users into court applications. So we're the front door, if you will, for folks who need to get access to the court data.

Di: Our understanding is that one of the first court applications that you are making available to county users, private attorneys, a variety of different users, is you're calling it the JUICE project. Tony, what does JUICE stand for?

Tony: JUICE stands for Juvenile [Information Content] Exchange. Really what it is, is an opportunity for changing the way that we've done business in the past. In the past, there were paper documents, particularly in the juvenile system.

Di: A lot of paper.

Tony: And those paper documents would be requested and then forwarded to either the social services or child welfare, public defender, etcetera.

[00:02:01]

So they were all getting information from the court, and then moving it around in a paper form, which had delays and is obviously very labor intensive.

Di: What's the vision for the JUICE project? What is it going to enable all of those stakeholders and improving the outcomes for kids in dependency or delinquency case types, what do you imagine this is going to achieve for all of those stakeholders?

Tony: We're very fortunate in that we have a judge in the juvenile system who is our leader of a blue ribbon commission [Orange County Juvenile Court Presiding Judge Douglas Hatchimonji], and what he's doing is he's coordinating with all of the other agencies, some of which you mentioned in terms of the district attorney, healthcare, child support, and what he's doing is working through all the issues so that the data is available. The vision is to change what is currently a three-day process, very paper intensive, very labor intensive, to an online instantaneous process such that a user logs into OCID and then is basically allowed, if they've been preauthorized, to get to the JUICE program and just launch it.

[00:03:11]

Everything becomes single sign on, instantaneous, with proper auditing and controls and policies around the access to the data.

Di: You've brought with you a diagram of Orange County and the Orange County Superior Court's long-range vision. May we ask you to describe this architecture?

Tony: Gladly. This diagram that shows Orange County Superior Court and how the two entities play together. On the left you'll see the public defender, social services, DA [district attorney], in addition to, but not necessarily shown here, other dependent agencies. They may not be government entities. This could be the independent counsels who are representing someone in a juvenile matter. Those are all what we would call potential users.

[00:04:01]

Those users go to what we call OCID, which is a portal. I also brought a slide that we can look at later on that. From that portal, those users, once authenticated with their prior granted rights, are then able to, with a single click, get into the JUICE system, which is again on the right, as a service provided by the court.

The diagram you see on the right is basically the local court users, [who] use the court identity provider, which is actually Active Directory. So those users come through the court Active Directory, and then get into the services down below, the service provider in this case, JUICE. And they have many others: we were talking about Banner, Vision, ELF, a number of others.

So this is extendable, as an architecture. The users on the left – which are non-court employees, non-court officers, in that sense, are basically county employees, and those associated with the county – will come through using the OCID as an identity provider.

[00:05:02]

So I think that kind of shows the two sides of this and how it interconnects.

Di: John, is there anything about this long-range vision diagram that you'd like to explore further with Tony?

John: Well, it just appears that in the diagram – and I just want to confirm that – each of these applications, the county services as well as the JUICE portal, etcetera, that none of those applications have users directly logging into those applications. Instead, you're passing a credential from either the OCID IDP [identity provider] or the court users on their side. So that separation of identity from the core application itself is, I think, a good model of what we have been talking about the last couple of days on federated ID and federation.

[00:05:59]

Tony: It also improves the security, because these applications are buffered and isolated within a data center architecture and are only connecting to known IDPs, as opposed to browsers that might be scattered across the world. You've got a much simpler security model.

The other thing to point out in response to what John's talking about is that these applications, several of them, are legacy applications, and they previously had direct access to them. But what we've done is, via the connectors that OCID supports, we are able to just move that legacy application behind the IDP. No programming changes, effectively, and it is transparent to the users.

John: So if you are defined to the OCID portal, and you are no longer working, say, for the public defender's office, then removing them from the OCID's portal as an identity with the public defender removes them basically from all of those various applications down below in one stop.

[00:07:10]

Where traditionally, the way we design applications, at least on this diagram, it would be about six different systems that you'd have to go to and de-provision them. That also is another security improvement because it's pretty unlikely that you can keep all of these different systems synched up with the current state of the identity that's been accessing them.

Tony: Part of the improvements and cost recovery on this is that streamlining of user provisioning and user identity. Within the County of Orange, we actually have a user provisioning and de-provisioning policy that articulates that within 24 hours, you have to have removed that individual from all of the directories and applications that they had access to.

[00:08:00]

Again, to your point, that previous was not possible. You couldn't have met these shorter time constraints. In this case, what happens is as soon as a notification comes in that the user has had a change in status, and there's many sources that could submit that change of status, then OCID puts that person on hold, gets a confirmation from a supervisor or HR [human resources] – again, many sources can confirm – and all of a sudden, they are de-provisioned from all of those applications.

The same thing happens also on the provisioning, by the way. Altogether we found that one of the leak areas was that a new person would show up, and the IT folks would – trying to help out – provision that person right away, get them into the systems, and then they'd need access to various resources, and they'd start putting them into those other databases. And so that encouraged a bit of the chaos. So, provisioning side, for new employees, they get provisioned once in OCID. We get a confirmation from the supervisor, and we get formal, auditable requests on what services they're going to need connection to.

[00:09:02]

It really makes it clean and streamlined.

Di: And accountable. So, Tony, as you've been working over the past several years to help Orange County move to this new model of identity management, what were some of the challenges that you encountered from your user community? Were they thrilled with this from the get-go, or what were the challenges in that change management?

Tony: I think our Orange County users are typical of every user, and that is ***any*** change is not a good change, so we had that initial reaction, "I don't like the change, regardless." But I think as they saw the value proposition, they've come on board. For example, and we'll go through this in a minute, in OCID, once you get an identity and you start provisioning, you have single sign on into all of these applications.

[00:10:03]

As we saw in this chart, there were six potential applications. Well, you don't have to remember six credentials; you only have to remember logging into OCID, one credential. They're starting to see the value of that. They're starting to see that if they need to get provisioned for a new application, whether it be inside the court, inside the county, or inside the cloud, that they just follow the OCID request form for change of access, and – *voila* – within a short period of time it appears on their launch list, and via a single sign on, can basically invoke that credential.

So they're starting to see the value of it, and we're getting way past the initial reaction of change is bad. They're now saying, "Hey, this is great. It's much faster, it's easier, and I don't have to remember all those credentials," which we all know is a problem.

John: Well, you just post the six or eight passwords next to your terminal, and that's how you can keep track of them.

Di: How secure is that?

[00:11:01]

Tony: I think all of us have experienced that one.

John: We've all seen it around the office.

Tony: There is an improved security as part of this, yes.

John: I think this also makes it possible to have stronger authentication controls, stronger passwords and enforcing that renewal. I, as a user, where before I had six or seven of these passwords that I was resetting through all these different applications, I only have to do it once. I can probably live with resetting my password only once and have a little tougher password that has letters in it and numbers and one character. I can probably deal with that when I only have to deal with one, but it was a real pain when all six applications were all asking for these complex passwords, or they'd say, "That password's not strong enough," and then you've got to keep it in your wallet or somewhere because you just can't manage that.

Tony: Especially in dealing with legacy applications, we found that.

[00:11:58]

Because some of the legacy applications don't allow you to use the same password that you used on other applications. Some of the user names for the legacy applications are different. Some even use your e-mail address, which is, *gee*, how hard is that to find? Again, and you'll see in the next slide, I think, that the design of the OCID portal was specifically to make it easy for the users.

John: So this is the unusual situation where both the security officer is happy and the customer is happy. Usually the customer is not happy with the security officer, but in this case, it's a win-win, so that's kind of an unusual scenario.

Di: For your user community, what kind of support did you offer that seemed to be particularly helpful? Was there training? Was there the idea that they would only have to remember one help desk number to manage their profile? How did you move folks forward?

[00:12:58]

Tony: With this project, much like other projects, the communication plan was essential, and it had to start early. Because this was really one where you're socializing a cultural change more so than some of the others where you're maybe just introducing a new application. This application changes the way you do business with all of your other applications, so it was very important that we have a roll out strategy.

The roll out strategy included many presentations. It included invitations, a monthly newsletter so that the community got up to speed on where we were going, were able to see the vision. We had envisioning meetings with a lot of the leadership. Then we actually did workshops so that as we rolled out to each agency, there was a short, ten-minute workshop in the morning, in the afternoon, the next day, so basically you could attend any of the short workshops, and in the workshop we actually went through how to log in and how to use it. People felt comfortable. They had seen it.

[00:14:02]

They not necessarily had touched the keyboard at that point, but they felt like they were aware of how it worked. We used in our demonstrations at workshops, we used the launch list, as we call it, for applications that they had a sensitivity to – timekeeping, payroll, things like that that they log into, and they could see, "Hey, I don't have to remember all those credentials. I can see the value." Then, we went back and set the expectation on, "We're not there with all of these yet for all users," but we were doing targeted roll outs.

Some of those were the success factors, and relative to the design of the UI [user interface], we actually, to your point, we actually did a lot of focus groups with users so that all the things the security officer might have liked didn't necessarily make it to here, but it was a balance because we wanted that customer adoption.

Di: So what I hear you saying, Tony, is that you engaged your user community pretty early. You gave them an opportunity to help design the interface. You communicated with them often.

[00:15:02]

Tony: Early, often, and endless is kind of how the team has said it.

Di: Early, often and endless. That's good. Did you encounter any obstacles with your user community that you didn't really predict? One possibility is that no good deed goes unpunished, and so you might already have a raft of enhancement requests that people now are clamoring at your gate. How is that going?

Tony: We saw that in the beginning with our first small agency, and we immediately thought of a strategy. What we've done is we accept requests through the program. You'll see on the portal, there's actually a feedback link. So we got the feedback links from the end users. However, what we set up was a quarterly release schedule such that the expectation was set that just because you put in the request, it's not going to happen tonight.

[00:15:58]

The expectation was that there's a quarterly release schedule, and that that implementation of the feature enhancement would not be lost in the tracking. All of those have been rated, and we set up a steering committee that was composed of important people within the agencies. Some of them are the folks who actually are the service owners of the applications we're servicing, and so they could see the feature requests. So the steering committee, as opposed to the project team, becomes the target for the user's appreciation or anger relative to that feature request didn't get done timely.

Absolutely that was a problem, and again, setting that quarterly schedule has helped us a great deal, and then having that independent body, that they're responsible for the ordering of the enhancements.

John: So just out of curiosity, this is early in the program, but looking forward, going through this portal, the OCID, and having your identity, and that gets you access to multiple applications, what percentage of applications that are typically used are still out there that they're still using individual credentials to access?

[00:17:10]

Do you think you've got some demand now being put upon those other applications for them to join and make their applications available via this model versus the traditional model that they provide?

Tony: Within the county, we have a steering committee on identity as a project. That steering committee was successful in getting the identity provisioning and de-provisioning policy through. The second thing that they were successful on was we have an "identity first" statement in the county. That is that any new applications will comply with identity and use OCID as the authoritative source for all new developments within the county.

John: You've actually institutionalized this model now, going forward.

[00:18:02]

Tony: So the new things coming forward have a priority. But to your other point, we have a lot of legacy applications. And although

OCID, our OpenIAM vendor supplied product, supports about seven or so different connectors so that it’s easy for legacy integration, that still takes a little time.

And so our priority is those new applications, working with those vendors, because some of the other legacy applications we know have a short life anyway: they’re being replaced by something else. Again, the strategy here has been: go forth with the early adopters, go forth with the feature requests, anything new coming in, we want to make sure it aligns to the identity portal. Then we take care of the more legacy apps.

[00:18:48]