[00:03:02]

Di: We are so pleased to welcome Tony Lucich, who is from Orange County, California. Tony, may we ask you to tell us your role in Orange County and why you're passionate about identity provision and technical privacy enforcement?

Tony: Certainly. That would be great. Tony Lucich, I am the County Information Security Officer for the county, and my responsibility is to oversee the security activities within all the agencies. In California, the court system is not part of the county. It's part of the state side, but I have a very close relationship with [Orange County Superior Court Chief Technology Officer] Snorri [Ogata], and the courts are a source of data for all of our county agencies, whether it be the sheriff's department, the DA [District Attorney], or social services. That's how we've gotten together. Relative to identity, for the last three years, I've been working on an identity project within the county.

[00:04:01]

Specifically, it's both tactical and strategic. The county of Orange is a mix of 37 separated agencies, and those agencies each have their own identity directories, repositories which they keep separate. Over time, just the simplest thing – as a common e-mail directory – it'd be nice if we all played together, so we began with that.

Since then, as resources and applications and databases are moving from internal within the agency, now cross agency, and as those data directories and repositories move out to the cloud, it's become more important that we have an authoritative identity, so that we can enable, provision, de-provision users into accessing those resources safely, securely, and meeting the regulatory requirements. That's been a passion. Tactically, it gives us that value. Strategically, it helps bring the county together.

[00:05:01]

And in such, we're able to reduce the number of databases we have, so instead of the DA keeping a completely separate set of databases from the court or from social services, what we'd like to do is allow those agencies, where regulatory allows it, to get a total view of a situation or a case. The example I think I've used before is you have a child welfare situation, and all of a sudden the

custodial parent is in custody. It would be nice to know that and set up the alerts so that social services, child support, and the sheriff all can work together to appropriately handle the situation in a timely manner, and you can only do that if you've got good identity.

Di: My understanding is that Orange County has a long history of working toward electronic information sharing. Is it fair to say that that started in the adult criminal justice business side of things? Or what is your understanding of –

[00:06:07]

Tony: We actually have two separate trains going down the track. Within the county, as I said a moment ago, we've got the identity and sharing. Historically, the court, the healthcare, sheriff, etcetera, we've all used a common data center, so that's the first point of sharing. The data center and my staff have acted as brokers, and we've brokered deals between the various agencies. So if the court had something that the sheriff needed access to, we historically arranged the network connectivity.

We might have arranged it for probation as well, but then we'd find another agency who didn't have – the assessor might not need it, so we would break that network connectivity. So hub and spoke, and we were controlling the kind of sharing that you were talking about at a network level.

[00:07:00]

So that's been the history behind sharing. And then within other kinds of sharing, we did a project in 2010. We did a project for e-probation where we did an XML [eXtensible Markup Language] transfer of documents between the courts and the probation department. We've done other kinds of sharing now of data exchanges between the DA and the courts. So that was the second train, the first train being identity and the second train being this identity and data exchange. What's happened now with the JUICE [Juvenile Information Content Exchange] project is they've come together.

We've found that with the new CJIS [Criminal Justice Information Services] rules and the need to basically authenticate each transaction with the roles and data access rights that that individual should have within that data structure, now we need that level of

granular identity. We need the identity provider and the service provider, and so JUICE project is the maturing of that process, if you can follow.

[00:08:00]

Di: Absolutely. That makes a lot of sense. I remember you saying that maybe it is helpful to understand Orange County's evolution in the idea that there had been this concept of network security and a vision of access control on the network, but now the business challenge that faces you and your colleagues in Orange County is that you need to drill down to transactions. Maybe you could speak to that.

Tony: To amplify a bit on that, the situation was network was fine five years ago, but now we're at a granularity where if I'm an attorney and I'm in the public defender's case office and I'm handling adult cases, I shouldn't be having access to juvenile, or juvenile to adult. So now within the agency, I can't just make that connection and allow it. I have to know who you are as an individual and decide what sub-systems you're able to get to.

[00:09:04]

Can you get to court calendar? Can you get to a sealed record or not a sealed record? That's really dependent on what cases you are on, with what role, within what agency, so now we're into identity and that level of granularity as an identity provider where the court records in this case would be the service provider.

Di: That's fantastic. John, do you have anything to add yet, or are you okay so far with this background conversation?

John: This is great. Just carry on.

Tony: We've been using a lot of the work that John and his team did in terms of the architecture and the key elements. Our identity solution follows very much the implementation of the [Global Technical Privacy] framework that was outlined in 2007, and we didn't find in the vendor community somebody who had that all in one box.

[00:10:01]

That's why the identity solution we've been pursuing pulls that together and then works closely with the identity solution, the different elements that the court's been using. Again, the two collide, and we've got a nice marriage there.

Di: Would you like to say anything else about Orange County's historical development to this key point in time?

Tony: I think there are some lessons to be shared with the difference between successful projects and unsuccessful projects.

Di: Do tell!

Tony: Do tell. As I said, I've been working on identity for about three years, and the exciting part about where we are today with the JUICE project is that we have executive alignment. We have the court officer for juvenile, who has basically become our advocate on this project.

[00:10:59]

He's reached out to all the other agencies at a high executive sponsor level and explained to them the value to the juvenile system, and to each of those agencies the WIIFM, "What's in it for me?" to each of those agencies. So now, we're seeing that. Again, we didn't have that before. Maybe the other side of that is now that we're able to demonstrate a working identity pilot, they're able to demonstrate a working juvenile data access element. All of these have started to come together, so I think one of the lessons learned is timing. The other is having that strong executive sponsorship. The third is actually finding out what the WIIFMs are for each of your subscribers.

Di: Regarding the JUICE project, are you speaking specifically about juvenile delinquency, or is it the entire spectrum of case types that the juvenile court hears?

[00:11:57]

Tony: It's everything in the juvenile court area.

Di: Abuse, neglect, guardianship, adoption.

Tony: Right.

Di: So this is some of the most sensitive data – among the most sensitive kinds of data in the public sector. What are some of the legal rules – or do you have some familiarity with some of the legal rules around who can and cannot access this kind of juvenile data?

Tony: Again, this isn't my source of expertise. But in provisioning the identity solution, what we're finding is that I now need to define those policies so that we say, "You have to be an active lawyer on this case to get this kind of data." So there's this whole, "Who are you?" is part of the question. "What does the policy engine say about what data you can get access to?" And then, "What does the actual data owner say?" which is the court side. So there are really two sides of the filtering. On our side, we filter once you've registered with an identity.

[00:13:02]

We call it O-C-I-D for Orange County Identity, as an authoritative identity within the county for access to resources that cross agency boundaries. Our user population includes folks who are not county employees. They can be contractors. They can be somebody working at a healthcare clinic. They can be an outside private party attorney who's involved in a case. So we have a lot of users or subscribers. Once you've subscribed, we then go through a process to refine that with your employer, who is your sponsor, we call it, to make sure that your identity is truthful, in that sense, building the reputation.

We keep intelligence information about where you access the system from, so we know a little bit about, from a security point of view, that you always come in from this IP [internet protocol address] in that building and during those hours. Now, if you do something different, we can set off some alarms inside the application.

[00:14:02]

But more importantly to the point are the policies. We know that that kind of an individual, being an attorney, or a case worker in social services who is on this unit within social services, which is the juvenile unit, then can have access to juvenile data on the court side. There's really that. Now, the court has its own rules engine relative to the data elements within the juvenile database, but really

it's the marriage of both having similar rules to get through the filters, and then you get the access. Is that –

Di: What has [Orange County Juvenile Court Presiding] Judge [Douglas] Hatchimonji presented as being some of the primary business drivers for moving to this electronic information sharing environment around the juvenile cases?

[00:15:03]

Tony: The judge is really looking at this as a streamlining of the current business process. He has followed and worked with his team, a blue ribbon team [Orange County Blue Ribbon Commission on Children in Foster Care], composed of business leaders in the other agencies that consume data through the juvenile system.

Di: Prosecutors, social services?

Tony: Prosecutors, social services, child support. Probation also is in there, DA, of course, and public defender. So what he's done is he's mapped out the needs they have for the data. He's mapped out that currently there's a lot of paper transactions.

Di: A lot of paper.

Tony: And so what the judge really set out as the vision was to enable a consumer of a piece of data, somebody who needed access to that information, the time it took, which currently runs about three days, because you request the information, then somebody prepares it. The documents get sent over. Typically a courier or somebody brings it on over.

[00:16:00]

So it can be a three-day cycle by the time you ask for the information and you got it. His first thing was, "I want to cut down the time it takes for you to get the information you need." He was very clear walking around the room and asking everybody in the blue ribbon meeting, "Are you all okay with this?" He got everybody on board that that was a goal they could buy into. Secondly he said, "And the time and complication we have – in a lot of these files are very thick, and getting it Xeroxed, multiple copies, getting it to the right person – are you all okay if we just get rid of the paper, and I could deliver it to you electronically?"

Most of the contributors to the discussion said a lot of them were scanning the document anyway. So we take it from the court where it might have been a scanned document, we print it, we put it in a routing with a Pony Express, and we get it to somebody. They then scan it back in.

[00:16:56]

The judge was very clear about the business process change here was speed it up, make it more efficient in terms of time, but also in terms of the paper handling and the security and privacy around the data, because once it's in paper, everyone in the room agreed that once it's in paper, we really had a hard time controlling it. His view was those were the metrics he really was looking at, and he went as far as saying he's stopping or curtailing the ordering of Xerox paper in June, and he wants us all to be on board that we're going to be doing data exchange, not paper exchange.

Di: So what I hear you saying is that it's really a two-fold business objective. One, and the one that's most obvious, is getting people timely access to the critical information they need to help improve the lives of these kids.

Tony: Three days after the event that you were asking about, that parent was in custody, let's say, it's too late. You needed the data in a timely manner and the current system business process – we've lived with it, but it isn't optimum.

[00:17:55]

Di: And the business objective that's less intuitive is that you are actually going to be improving the privacy and security for the citizens and the parties who are involved in this case.

Tony: We'll have the audit trail of who had access to the data. We'll have the ability to say what parts of the data they got access to, what parts may have been redacted. Given that the paper system is what everybody's been used to, a lot of times they said, "Well, I can't share this document with you because it's got all of this in it." As we move more and more to a data structure than a paper structure, we can pass over those five elements of data that you need and you have access to, and we don't have to worry about trying to redact each document personally because you might need something different than John. We can send you each the data elements you need in a timely manner.

John: That's common also in drug court management systems where you have drug court ordering treatment.

[00:19:02]

And the treatment providers need medical information. They're not privy to having some of the court criminal history information on those individuals. So again, it's just another illustration of when the information is structured, you can have policy for what the drug treatment providers can have different than the policies that the managing probation officer has.

Di: Without the big, black Magic Markers.

John: Yeah, without all that on the paper.

Tony: And the pair of scissors.

Di: So in terms of business outcomes, what Orange County is predicting – if I can just put words in your mouth here for a minute, Tony – you're predicting better outcomes for kids and their families, and you're predicting more efficient business processes for all of the service providers in these children's lives.

Tony: And better control over their privacy around that data and those transactions.

[00:20:05]

Di: So let's move then to make sure that we understand, how are you governing this project? You mentioned that there is a blue ribbon team, a blue ribbon commission maybe, specifically Orange County stakeholders.

Tony: Around the juvenile JUICE project, yes.

Di: And could you tell us a little bit about how formal or informal that governing body is? Have you executed MOUs [Memoranda of Understanding]? How are you moving forward with some of the formalities?

Tony: The blue ribbon commission is really acting as a steering committee, not as a legislative type commission. What we in the county are doing is preparing MOUs to relate the relationships.

[00:21:00]

Now within the county, we already have agreements relative to how the DA and the public defender, etcetera, all interact. What we're really creating is the MOUs that'll describe the relationship between the OCID community of consumers and the court as a resource provider. We already have a number of MOUs. Again, an advantage for us is that because we were sharing the common data center, we already had some MOUs in place that described the relationships on a very infrastructure basis, and now we can talk about it on a data basis, a data exchange basis.

So we're amplifying that up, and those MOUs will become more of our authorization, our official correspondence. Then the judge is drafting some language about his data exchange relative to how he views that will be handled.

[00:21:58]

Toward what John's talking about, we'll end up getting agreement on the policies, the rules engines on both sides so that everyone has an expectation of privacy and who has access to what kinds of data.

Di: So you've got a blue ribbon commission that is acting as the executive steering committee, identifying potential barriers, finding solutions for those barriers, achieving that buy-in. Do you also have some inter-agency working groups that are going to be specifically tackling technological issues or policy issues? Tell us a little bit more about those working groups.

Tony: The blue ribbon steering committee really is holding the vision around the data exchange of juvenile information, around the JUICE project in its rollout. We also have, for the identity solution on the county side, we also have a steering committee about the identity manager.

[00:23:03]

That steering committee again is composed of representatives from the various stakeholder agencies – not all of them, but certainly the representative ones of the DA, the public defender, healthcare – who have probably the largest regulatory challenges around data sharing. JUICE is just the first of the data exchange with the court.

We have many others with the court, plus we have a large number of data exchanges that are established for other elements, where probation officers would like to see some healthcare data from the clinic, but only certain fields.

This isn't really a one stop, one solution. We intend to replicate this, just like we're doing juvenile data, with other data that is needed by the same community of users.

[00:23:55]

Di: So you envision that this architecture, the identity provision and then also the fine grained authorization, this is going to be an architecture that's going to be scalable for many of Orange County's future information sharing needs?

Tony: Right. Our current user population that will be using the identity solution is about 26,000.

Di: Wow.

Tony: Which is huge.

Di: That's scalable.

Tony: That is intended to include the private attorney sector, who need access to criminal data. It includes many clinic workers, who need access to healthcare data. Again, in each of those transactions, you want that policy engine acting as the broker and audit and security to make sure that the right people are getting the right data in a timely fashion.

Di: Are you aware, Tony, has there been formal county ordinances or formal legislation supporting the creation of OCID or the blue ribbon commission, or was this more just a coalition of the willing, as you might say?

[00:25:04]

Tony: Well, the coalition of the willing got us a long way, but after two years we finally got a county-wide user provisioning/de-provisioning policy that was approved by the executive steering committee, which sits underneath the board of supervisors. Again, there are often times that we wouldn't take something to the board, because we want the policy to be flexible, particularly on

something new – new for us, I should say – a county-wide provisioning and de-provisioning policy where you know you might need changes to it. There is the policy piece on that side. I know on the court side there are some internal MOU documents about JUICE.

Basically the blue ribbon is keeping the vision and helping clear the way, but behind that we are doing things that will be documentation that will be policy regulation internal.

Di: For all county agencies.

[00:26:02]

Tony: For all subscribers to OCID.

Di: Oh, good point.

Tony: Because remember that includes people who aren't county employees. It includes contractors, people who are under business associate language for HIPAA [Health Insurance Portability and Accountability Act]. It includes attorneys who would be logging in as long as they are associated with the case. Again, there's the cross check to make sure that you're still on the case today and you should still have access today, so provision and de-provisioning, as well as technology user acceptance forms, the standard security awareness courses. Those are all part of the thresholds or obligations that people who use OCID must meet.

If you get a driver's license, then you also have to be able to drive the car and pass the test. That's a simple analogy.

[00:26:47]

John: I'm just curious if someone like state corrections, for example, needed access to some resources that you have there in Orange County, and they have a large group or a large population of users that they provide the provisioning for and the identity management for, how would you incorporate them into providing access to their identities to some of your resources?

Tony: The question really comes into who is going to be the broker. If the state corrections was to approach the court, the court might act as a service provider if the state corrections had their own identity provider, so that relationship could happen that way. Another way

it could happen is that the state corrections could come to us as OCID and say that, "We have a population that we will vouch for, and we will follow your rules about becoming a subscriber to OCID," and through OCID they could get to the court where we're acting as an identity provider and the court again is acting as a service provider or a resource provider.

[00:27:57]

Our requirement on OCID is that we have a mechanism by which we can validate your identity, that somebody is your sponsor, and that that sponsor has a legal relationship to keep your information up to date. There's the carrot and the stick: "We'll let you in, but oh, by the way, you need to agree to make sure that your data is up to date."

So, for example, our current situation is very simple in that the requestor can say, "I'd like access to the data," whether it be payroll data or justice data from the court. Their supervisor has to say, "Yes, that's okay with me." Their local security administrator has to say, "Yes, it's okay." Then the end user, the owner of the data, the data owner – in this case, say, the courts – has to say, "Yes, that's okay," either as an individual or by policy. So if it's by policy, it might be all correctional officers working on this piece of data having that functional role are allowed to have access to this. So we would get signed approvals by both sides.

[00:29:06]

John: So the court could have an agreement with an identity provider at corrections, or the identity provider at corrections could have an agreement with OCID to –

Tony: To trust their identity.

John: To provision their users, basically. And then, through that mechanism, access it. So there are different configurations.

Tony: You're raising a good one. The difference between what was originally articulated and what we're implementing is that we're implementing a full-service portal. So through the self-service portal, I have all of my personal contact information, emergency as well as regular, my credentials, my applications. So I'm able to launch, off the self-service portal, multiple applications.

[00:29:58]

I can launch Salesforce Box, Google, JUICE. I can launch my VTI [virtual Texas Instruments calculator]. What's in it for the users was to make it simple. We did a study in Orange County. Currently, people are keeping 15 to a ***large*** number, but averaging more like 15 credentials.

Di: Per user?

Tony: Per user. They would love to go to a more simple dual sign on. We try and avoid the word "single sign on." Because somehow you got on your laptop. You got on your local LAN [local area network]. That doesn't count. But once you're on there and you're into OCID, then it's a simple launch for everything else.

So this is our value proposition to our end users is not just accessing the data, but making it in such a simplistic format that you can launch the applications.

Relative to the service providers who agree to work with us, there's a value to them in that previously you might have had a 30-day refresh on your user names and passwords for your private repository.

[00:31:02]

Once you allow OCID to become your connection point or your trusting of the identities, OCID is the only one who knows the users and passwords, so you have to log into OCID. Once you launch it, it uses what it knows to be your credentials to get into the next system. So this improves security tremendously because I can't write down the password. I can't give it to you because I don't know it. Only OCID knows it. So again, there are improvements from the end users' experience, plus there's a lot of security improvements.

John: This is a theme that I think we even heard earlier from the Connect project, that it was far more productive and even performance was better by establishing a portal, and your credential against that portal is where all of your identity attributes, if you will, are then passed on to the different resources that you have access to.

[00:32:04]

Even what's presented to you as the resources you have access to uses your credential to see what you can go and get to. Now all the resources just need to trust the portal's identity as well as the identity provisioning and provider attributes that are coming to it. They don't have to set up all these multiple relationships.

Tony: It's a real win/win.

John: It's an efficient way of doing business.

Tony: It's simpler for the service providers. It's much simpler for the end user. They don't have to keep track of all the different systems.

Di: Fifteen credentials.

Tony: And as we move forward into this anywhere-anytime computing model – or what we call "security without walls" – this is essential, because the paradigm shift of being able to control your workstation gets to your database is gone.

[00:32:57]

Where we are now is anytime-anywhere means that I might be on my iPad, and I could be in Williamsburg on my iPad, and it needs to know that that's okay to let me into a cloud application, which doesn't even go through the data center. So by going through the portal, I get that audit log of who went to the cloud. I get that audit log that it was really my iPad, and so the confidence level that it was me is higher. So you see there's tremendous simplification of the interface, but a lot more security behind it.

Di: So what I hear is another important business driver, Tony, is that OCID is making mobility possible for the staff and the associates of Orange County, who could do a much better job if they were out in the field rather than stuck at a terminal in an office somewhere. Could you talk a little bit about – I mean, you have, but I really want to drive home this point that your model enables mobility.

[00:34:04]

Tony: It is built around that concept that we can no longer depend on knowing where you're coming from in terms of a location or knowing that you're coming from a controlled computer, because you could be on your iPhone, your iPad, etcetera.

So we historically put laptops inside the cars for our probation officers. We then had to move them out of the cars because the probation officers were making house calls. So now we've got this with encrypted data on it, but he still needs access to records that he's not carrying with him. So do we let him directly into our probation database? No. We need to find out that it's really him at the end of that laptop and not that he left it somewhere or that somebody else got his credentials. Things in OCID are pop-up questions. If you're coming from a device that we don't know, you'll get that pop-up question that challenges you to validate that it's really you at the end of the terminal.

[00:35:06]

So there's a lot of security intelligence built into it.

John: It's basically being managed at this identity hub, this OCID, as opposed to every single application out there each having its own version of how they're going to authenticate you and what credential they're going to require for you.

Tony: In terms of credentialing, another simple way to view it is if I'm sitting at Starbucks, and I'm logging into a website, those credentials are transported and so are a lot of other data elements. From OCID's perspective, I'm logging into OCID securely. It then has a variety of ways it can connect to the back end databases, but it's only OCID to the court system, so we can lock that connection down tight. It's not anywhere in the world to the court system.

[00:35:58]

So those back end connections are much cleaner from a security point of view than when you allow any user coming in through the public internet to get anywhere. It's all funneled through the OCID and Connect. We've had to build a robust cluster so that it can basically handle the load, the DR [disaster recovery], and all of those sorts of things, because you don't want it to go down.

John: It becomes a secured gateway, if you will.

Tony: It is a gateway, yes.

John: And you can put a lot of controls there that you can't really put in all those different twenty resource places.

Tony: Some of the other solutions we looked at were, "Great, we'll put a particular client on your laptop. We'll add some software to your –" We can no longer use that model because it's any kind of a device at any time. I could be borrowing your laptop and still want to get in securely.

John: I get my e-mail on my iPhone. I get my e-mail on my laptop at work. I can get my e-mail pretty much on a variety of devices, but I have a particular authentication that's always being done against the central organization's directory.

[00:37:09]

Tony: And we avoid downloading the data to everybody. That was the other thing we looked at in our use case analysis was we had instances where everybody was bringing pieces of the data – the secure, private data – down to their devices. Now even if it's an encrypted device, now in terms of keeping that data up to date, I've got copies all over. Whereas really what I wanted to do was let the end user get to the data they need. They didn't necessarily need a copy, but because it was so cumbersome to get to, they'd keep a copy.

We did a use case analysis of over 130 use cases, and each thing we did was to simplify one of those.

[00:37:45]