Di **[00:00:07]**: So we have been talking with Tony Lucich about Orange County identity provider, OCID, and what we'd like to do now is focus on some of the screenshots that show what that user experience is. Just to underscore, these are county employees, but they could also be contractors with the county, private attorneys who represent parties in litigation in the county, a wide variety of users, not just county employees, right, Tony?

Tony: That's absolutely correct. Although we're focused today on court primarily, we also have an area of healthcare – folks who [are] contractors, entities, etcetera, through business associate – who have access to healthcare records who go through our identity solution as an identity provider for that kind of a record as well.

[00:01:01]

Di: What that's enabling is your county's compliance with the Health Insurance Portability and –

Tony: HIPAA.

Di: HIPAA [Health Insurance Portability and Accountability Act]. So what we've got here is a screenshot of the – maybe the screen that opens up when someone invokes the OCID portal?

Tony: The slide we have in front of us, the "What does OCID look like?" slide, basically is a screenshot of the portal. It is an identity management portal, so basically it's an identity provider designed to connect to other service providing applications, whether they be in the cloud or in the data center. The thing that makes our OpenIAM solution called OCID unique is that basically a couple things. One, it implements the justice document, which was – the one I have here is the 2007 implementing privacy policy [Global's Technical Privacy Framework].

[00:02:01]

We use this really as our backdoor Bible for the design of OCID with our vendor and also the direction for when we came down to putting in the rules engine that is associated with policies.

John: Policy authorization.

Tony: Policy authorization and the rules that policies make up a rule, etcetera, coming across. But we also found that for the user

feedback and engagement, it was important we added a number of other elements to the portal because we needed reasons for them to go to a portal. We could have done – and many times an identity providing solution doesn't have the full portal. They're just a link.

What we wanted here was to provide a more rich experience for the end user. On the screen you'll see that – of course, in the upper left there, we've got the log in block. We used a credential called a UPN, which is a user private name. It's not your e-mail address. It's not your network log on in the morning, your username through Microsoft or whatever your log on is.

[00:03:02]

This is a user private name, a UPN that is unique to OCID. Again, we were trying to avoid confusion because in our initial piloting with our users, we found that they didn't really understand single sign in. They were looking for how to make sense out of it, so we really wanted to isolate the credentials that are OCID universal credentials separate from anything associated with your other applications or your other network.

The other thing we use is a pass phrase, and the pass phrase sets the expectation that it's not your password, and it is a phrase, meaning it's longer and more complicated. That allows us to increase security because our two credentials are not something you can guess or look up by e-mail address or guess by first initial last name as a username, so that was part of it.

Then, obviously, below, we had to add the self helps links such that if you forgot your UPN or you needed to auto reset your password.

[00:04:00]

Again, part of the cost recovery here was based on the fact that we eliminated calling the help desk. We eliminated the help desk having access to your password or changing it. This is all through the identity solution.

There's a news box down below, of course, for information relative to system updates and downs. But more importantly, the self services column there on the right, where it says access management, reporting and self service, those features really were things that the users said they would like a portal to provide.

We provide directory lookup, so we can put you in touch with any user who is an identified user. That meant it was important for you to keep your phone and location up to date. Others are going to use it. We also included in that directory link a feature that was a feature enhancement from a user that said, "I've looked it up in your directory and it's wrong. That's not their phone number."

[00:05:00]

So we actually allow that someone could submit a change request for your phone number. Again, this creates this community around OCID in keeping the data up to date, and that was important to us.

Of course, we've got the standard challenge response that you would find for forgotten passwords. We have a feedback and support link that's built in. Again, we talked a little bit earlier about any user suggestion gets put in the queue, and then it's managed by a process for our quarterly updates.

The change access portal also does user provisioning and access roles, so you can go in and basically say, "I would like to put in a request for access to a new system." It might be JUICE [Juvenile Information Content Exchange]. It might be AIM – or ELF, rather. So basically the user can make the request. Provisioning and entitlements are done through this portal. If you request access to a new system, it manages the entitlement that you would get for that, similar to what we had talked about in here as a policy administration and policy identity rules engine.

[00:06:05]

What happens in OCID is it front-ends it with a workflow. So the user can request access to a new application. His supervisor approves it. It moves to the owner of the application, and if they haven't given us a guideline of who gets in and out based on attributes, then an e-mail is sent to the owner of the application and they get to approve or deny that individual's request. It's all automated.

John: This is how then the attributes aren't set by the user, but the attributes that are required once approved will now be associated with that user. Once the supervisor says, "Yeah, that's a role or the type of individual that we would grant access," and then that's provisioned.

Tony: We have some applications where the identity solution and the provider have agreed – the resource owner, we call that – have agreed to it.

[00:07:01]

So, an attribute might be the division you work in. So if you're in the public defender's office and you are assigned to the juvenile caseload, then that immediately – those attributes are defined and validated against your organization, both your supervisor and HR [human resources], we have multiple cross feeds – so those attributes are associated with your record in OCID.

Then those become entrees for when you would request access to, say, JUICE, the juvenile system. It's going to say, "Well, we know that that is a legitimate request because you're part of the DA [district attorney] who has access or the public defender. You're part of the juvenile caseload group, and so we think that moves along in the workflow." So, it's automated in the workflow based on attribute, just like you've described.

John: So after you authenticate here, does the resources that I'm authorized to access, does this portal provide that list to me?

[00:08:01]

Tony: Excellent question. Moving to the next slide, which is the second slide, "What does OCID look like?" This is the one that shows on the screen once you've logged in. This is what you'll see. The center block is a block about the information we have on you, so this again encourages you to keep it up to date.

And at the bottom, you see the county usage policy. This is a policy link that when you click on it, it takes you right into policy. You agree to the compliance: in this case, the usage policy, as part of a constraint we have that you can't use OCID without having agreed to the policy. So it's online policies, in this sense. We have, in the case of law enforcement, there's like three of them that show up. If you're an officer, you have CJIS [Criminal Justice Information Services] policies, etcetera.

So you will have complied with those. We date and timestamp the agreements, so basically this makes you a valid user.

[00:09:01]

The context to your question is on the left bar, where you see those enterprise applications.

John: In the box is what's available to me based on my attributes and the policies of those various systems.

Tony: And those are live links. The way that we've implemented, these are launch links.

John: So click on it –

Tony: So you simply click on JUICE. It knows all of your credentials for JUICE. It also knows that you qualified and through the entitlement process were granted access to JUICE, and it passes those, in this case via a SAML [Security Assertion Markup Language] exchange, to the service provider application, which is JUICE, so we have the identity provider talking with the service provider. It's all transparent to the user. It is single sign on, for all intents and purposes.

So as you request an application through the manage request screen of the portal, it gets approved. The next item appears on your launch list, so it's very transparent to the user.

[00:10:00]

John: And so what was one, two, three, four different log-ins and passwords is now just a click after I've logged in once to the portal.

Tony: So from the user's vantage point, they'll trade four or five credentials that are all different formats for one credential that is a little more challenging.

Di: Well, let's expound on that benefit to the user community just a little bit more. Imagine that I am a child welfare case worker. I'm out in the field in Orange County. I'm conducting a home visit with one of the children that's in my case load. Can I access these kinds of things through my mobile device?

Tony: Yeah. One of the other features that using the OCID portal, the way that OpenIAM implemented it, is that everything is through a front end proxy. It just requires a web browser. Basically you

could go to your iPad or Android, open a browser session, authenticate to OCID.

[00:11:05]

It's a secure portal, and it will then create browser session for you for JUICE, so it maps the application through a browser screen, which maybe that legacy application wasn't really browser friendly. So we get that advantage. To your point, yes, in the field you can be using your mobile device to get to these applications securely, audited. We have a feature on some of the applications that are more sensitive in their security nature that it actually keeps a record of the screens and the inquiries you did, which we didn't have before.

John: So logging – audit logging.

Tony: It's audit logging. Some of the legacy systems didn't have the logging that would meet the new compliance regulations.

John: So you can provide it here.

Tony: Right, because it's acting as an intermediary or a proxy, you're able to audit all the transactions. And we know where you came from. In other words, the IP [internet protocol] address and the device code on your mobile device is also captured.

[00:12:03]

Di: Another area of great interest, especially in the juvenile community, is this idea that while the case worker is in the field, there's important data and information that they need to collect and that needs to be validated, maybe through geospatial coding or something. Do you imagine, Tony, that it would possible, for instance, for me to take a photograph of the child that I'm visiting and have that be GIS [geographic information system]-enabled, data- and time-stamped, and then fed into my application without me having to go back to the office and upload it? Can you talk to that advantage?

Tony: That kind of capability is certainly within the realm. We have an application in Orange County through the sheriff's department that tracks graffiti across the city, and it uses – they're currently using an iPhone, although with the OCID portal you could use the portal to get to it.

[00:13:08]

So the graffiti application basically tracks the actual gang sign, the location, the GPS [global positioning system] location, etcetera, and then feeds it across to the application, and that can go through the OCID portal. That's an example, I think, that has less around authorization of who could take what photos of children, but it's very good in terms of the graffiti and the signs because immediately you see where gangs are changing their territory. And from a GIS perspective, you can see the boundaries, and all of a sudden you get graffiti out of that area, and you're able to track it back.

So there's a wealth of futuristic ideas and devices that this portal will support because it's basically built on very core standards and ensures the privacy and the policy rules are being in effect throughout.

[00:14:00]

Di: So let's take a moment now, then, this is from the user's perspective and as you were saying, Tony, one of the big benefits for the user community is that it is transparent to them. They need not understand or don't necessarily even care all the magic that's happening behind that little box with all of my list of applications. But ***we*** care. So if we could pull the curtain back on OCID. Let's move to the system diagram that's labeled "OCID." Could you talk us through how you make this magic happen?

Tony: Sure. Again to reiterate, what we did working with our vendor, OpenIAM, was really implement what the justice information sharing framework was. They had already been doing identity for ten, twenty years, so it was great when we brought this document to them because they were able to match up their experience with the framework that was provided. We found some names where you would call it one thing and they would call it another.

[00:15:03]

They have a rules engine, and of course, you'd say policy administration, and you have the PDP.

John: PDP, policy decision points.

Tony: They had different terms for it, but the exciting part was that they were able to come together pretty quickly to building blocks that work and are compliant with this spec and allow for some future ideas.

So this is kind of under the skin. This is a block diagram. I guess going through the block diagram, the top level here is the user interface and what we showed here is that the out-of-the-application interconnects are basically a standard browser interconnect.

We have the ability that – The program supports APIs [application programming interfaces], so if somebody wants to write code to directly talk to the internals of the engine – So if you have an application that basically you want information in or out of OCID, following the policies, and you're not really a user, but you're another application –

[00:16:05]

Di: System to system.

Tony: System to system connections are supported. I think our focus is really about the user community, but the APIs exist, and there are several hundred of them for system to system connections.

The other thing is that basically it supports messaging through e-mail, through SMS [short message service], other kinds of structures. A simple example of that is if you are set for a particular kind of password reset, it will send it to SMS to your phone, so there's a code that gets set as part of a password reset.

John: It lets you know it by multiple distribution channels.

Tony: The other part of it is that, again, we do support a workflow engine, and through the workflow engine if you had a request that had been pending for a period of time and you hadn't logged in, a reminder e-mail would be sent out to say, "Hey, log into the portal. There's someone with a pending request you might want to look at," that kind of thing.

[00:16:58]

John: So this is for the administration of the IDP [identity provider] itself, this workflow is just a structured process to update – you've

changed your role, you've changed your job – this is the way to get those changes reflected in the identity provider.

Tony: Right. When we talk about workflow, if you go to the middle tier here, you'll see that the identities, your profiles, and then the provisioning workflow. I probably should have said provisioning workflow because clearly it's not associated with the rules or the policies. That's a separate process, as shown with the other databases and life cycles.

Basically going to the internal logic layer where the business logic for the application OCID as an identity provider exists, you have reconciliation so it does an ongoing process of using some security intelligence to make sure that the credentials are valid, that they're current, that we're not giving access to someone who's basically left the organization.

[00:18:01]

We also keep track of when you last activated logging into different applications, because if you haven't logged in for a period of time, it may be you no longer need that application, so we'll try and condense it. It can actually disappear from your launch list. If the system owner has set a short timeout and says, "If it hasn't been used in three months, take it off the launch list. Let the user re-request it." Again, because it's single sign on, it's relatively easy to do a lot of that.

Request processing, OCID supports not only access to applications, but it also supports controls of laptops, phones, etc. One of the things as security officer I found was that we had individuals who might be separating from the organization or changing roles, and it was also embarrassing to say, "And do you have any keys? Do you have a laptop that was issued by us?"

Di: A mobile device?

[00:18:59]

Tony: A mobile device. Because those records were kept in IT asset control, maybe, maybe not, so OCID, one of the functions we added here is assets.

John: I like that.

Tony: Because the mobile device, now, asset is actually linked into the network. As we start moving down that road, that credential on that laptop or iPad device might actually let you in, and it might be a valid device credential that we wouldn't want out there. We want to recover those things. After you've been separated or changed organizations or roles.

So this gave us requests that are accessing applications, devices. It really allows you to manage the whole user experience. Process execution, messaging, and provisioning are really around the user experience.

[00:19:48]

Skipping back to the process requests, if I request access to an application, I will define the application and the role I anticipate having, whether it be a criminal justice role, where I would say, "Gee, I'm a case worker, and I need to be able to update and change, edit, approve. I need to be able to submit new information." So OCID supports, I think it's seven standard roles, and those roles are then mapped to the application.

John: So is there like a drop down? And they can say, "My role is," and click on that?

Tony: Right, and in working with the application owner, the drop down is associated with that application. So when we register the application as an available link that you could auto launch out of OCID, we have a discussion with the application owner, and we map our standard roles to their individual application roles, so we can move that request along. Those roles allow us to decide what policy makes sense for that individual.

[00:21:00]

Tony: The policy about the application. Those policies then have individual granular rules within the application. We try to make it as simple as possible. The user just needs to know their role. OCID understands roles mapping all the way down through the policies and the rules. But that's transparent to the individual.

Those databases are reflective of really how we do view this. We've spent a good deal of time with the vendor developing a set of tables that reflect the policies and the roles and rules. The reason we did this is that we're looking for reusability. One

criminal justice application might have the same policy as another, and it speeds our integration time.

So the whole thing here was to take the statement that most people say is, "Oh, that's a legacy application. It's very hard to integrate."

Di: It is a big concern.

[00:22:00]

Tony: And what we've found is that's a fallacy using this application approach, in that it may be hard to integrate, but does it talk AD [active directory]? Does it talk LDAP [lightweight directory access protocol]? Great, so the connector is in place.

Are the roles, and hence the policy rules, similar to some other application? We have Court Banner and Court Calendar, which are very similar, so basically we'd reuse the policy and maybe tweak a rule or two.

But again, the whole idea was to speed up that integration time.

Di: So what I hear you saying, Tony, is that when you bring on a new application as a participant, as a service provider in OCID, you are not starting back at square one every time. You are trying to reuse as much intelligence as you've already developed for other applications

Tony: We're leveraging the standard connectors. We're leveraging the standard policies and hoping that a policy already exists in the list that's similar to what you need for your application.

[00:23:02]

And we're leveraging the common identity and the common portal. So basically it speeds that whole process. Our intent was to have integration happen with no coding, recoding or very, very minimal recoding. Again, that's part of I think a fallacy that many people have, and that is, "Oh, if you're going to integrate it with a portal, you have to start from scratch. It's going to be a redo [of] the application." No, no, this is relatively easy.

An example of that is we have an application in the county that does timekeeping and keeps the user repository information in its internal table. It happens to be a SQL table. They said, "Oh, we're

not rewriting the whole thing." There was a lot of hubbub about that with the author and the owner of the code. We said, "Great, SQL table. Great! Can we have access to the SQL table for some testing, etcetera?" That night, we just connected to the SQL table with OCID's connector, and the next thing you know I'm going, "Okay, well, we've provisioned the user. Look, it changed it in your SQL table."

[00:24:01]

So it's very simple as opposed to the traditional concept where everybody's fearful of code change.

John: So these access control policies, you're actually storing them here in this PAP, policy administration point?

Tony: Right.

John: And then the PDP, the policy decision point, is – basically, when the user clicks on JUICE, it's going to go down and it's going to pass the credential, and it's going to consult the appropriate policy from the policy administration point, and then that policy will be executed by the PDP, and then they'll either get into the proper role or etcetera.

Tony: Right. We explain it to our community as a filter. When you come in and you click on the launch list, you start at the top of the filter. The filter is going to check to make sure that you're still – by your attributes, the organization, the division, your role – you're still qualified to go to the next level.

[00:25:06]

And eventually you're coming down the filter through the policies, both the decision point and the administration, and then it says, "Great. I'm going to hand you off now to the application JUICE," and on the JUICE side there are also policies and rules, as your document defines.

John: So the actual services that they're getting to aren't really on this diagram, but the path to get there – the very bottom, if I wanted to go back to an earlier diagram you showed us, that's where I'd put county applications. I'd have JUICE, and I'd have all these other applications.

Tony: Court applications and cloud applications.

John: So I guess in terms of a flow from top to bottom, underneath the connectors is where the actual service or applications are that you're accessing.

Tony: This is really kind of an internals of the application, and you're right, those connectors would hook out to the standard network to wherever it is in the globe that that service is running.

[00:26:06]

John: Thank you.

Di: We have reviewed the big picture. We have reviewed what it looks like from the user, a very simple user interface. We have explored, with this last diagram, the connections between the IDP, the PDP, the PAP. Is there anything else that we would like to bring forward at this point about Orange County ID or the JUICE project?

John: I think when we look at the overall privacy policy network, there's another component, which is the policy enforcement point. I think it's fair to say that the policy enforcement point is at the point that those credentials are kind of passing through this first layer, right?

[00:27:04]

Then the policy enforcement point is really directing that to the PDP, the policy decision point, which is pulling up the appropriate policy and running through those rules and then, from there, letting you get to the particular service. The connector is involved in that policy piece.

So I would just say that if we were trying to related this to the overall architecture, the PEP [policy enforcement point] is really happening in this data use to the right here where the PDP and PAP is, and the connectors, and then the resources are exposed.

Tony: I think you're absolutely right. If you took where the box is labeled "business process execution," that's really the PEP that feeds into the PAP and the PDP right here.

John: Right, that's the hand off.

Tony: And that's really the hand off through that execution of the policy.

[00:28:02]

Di: Now that you've got us thinking about this, John, Orange County does not necessarily have a single PDP. So in other words, a user who wants to access JUICE, actually that PDP has been stood up and will be maintained by the superior court next to the juvenile case management system, right?

Tony: There are two sides to it. There's the part that's inside of OCID as the identity provider, but there's also the wrapper around the actual application inside the court. So what's making it easier for our integration activities is that as I define with our team our policy rules engine table on this side, we're actually exchanging the table with Snorri and Danny's team, who is doing the JUICE program, and they're using the GFIPM [Global Federated Identity and Privilege Management] modules on their side.

[00:29:06]

We are using, of course, our OpenIAM Java modules on our side, but we're both basically maintaining tables. So what we're hoping is to find some simplicity in that exchanging those tables makes it easier to develop the code, because we're finding the fields, and we're really categorizing it as very detailed granular rules that are at the data level that build to a policy which is a collection of those rules. And so there are really two separate activities around this.

Di: Anything else, gentlemen?

John: Well, the other piece I would just say is that up here where the user is in the UI [user interface], if you follow that all the way over to the left, that is the identity provider. The processes of the actual authentication are happening up there at the very top where the user is.

[00:30:01]

And their attributes are being stored in this identities database that's on there. So again, that's just kind of tying the pictures together. You had an IDP that has attributes about those users. The IDP performs the actual authentication step, and then you pass that through the business process execution, and then the authorization at a high level is performed within the OCID

environment, and then that credential is passed down to the particular service provider, and then they have some additional policy rules that get applied. So it's kind of like there's a gate keeper for some high level policy, and then as you go down. If I have captured that accurately –

Tony: That's captured accurately and correctly in sort of mapping this out. And one of the other things that that's enabling us to do is via the connector, in the case of like JUICE, we pass I think it's 10 attributes across.

[00:31:04]

Which then get reevaluated on the JUICE side of the policy administration to make sure those attributes still validate that this is the right person. It provides auditing and other things.

John: Sure, they have to do their own logging at the application level.

Tony: Their own logging on their side.

But the other thing that's happening is that in the case of legacy applications, we map your credentials across because each service down here that's connecting to OCID may have a different username – well, they ***will*** have a different username and password and other credentials. So as you connect up through the integration, without coding, we're basically targeting in our registration screen what attributes do you need passed? Do you need a username, an attribute? Do you need a division? In the case of JUICE, they want to know that you're in the juvenile division.

So basically you can customize from the pick list the things that get passed across, as well as the connector that's used for that.

Di: And the user, from the actual user's –

[00:32:01]

Tony: It's transparent. They don't know and really don't care.

Di: Right, nor should they.

Tony: Nor should they. The idea is to allow them to get access via the launch links to the systems that they know have the information.

And I think in terms of the future at some point, some of those system to system connections we talked about will basically allow that he'll click on one, and it'll do a mash up through the OCID portal of that information, but we're not there yet.

John: I really like the combination of the authentication and the IDP and the portal all being in one stop, and you can see all the applications that are available to you in this particular federated model, as well as do one authentication right there at the door. You don't authenticate in one place and then go somewhere you have to remember where all the different resources are and go clicking on all those. That's all been brought together. I think it's a good design. Great design.

Tony: Thank you. We saw some systems that did it the other way. It was – certainly it accomplished the goal.

[00:33:04]

John: Technically either way can be done.

Tony: But it was clunky from a user's perspective.

Di: You really want to drive traffic to OCID, so you had that value proposition for them.

[00:33:15]