**Remote Case Access and Identity Management**

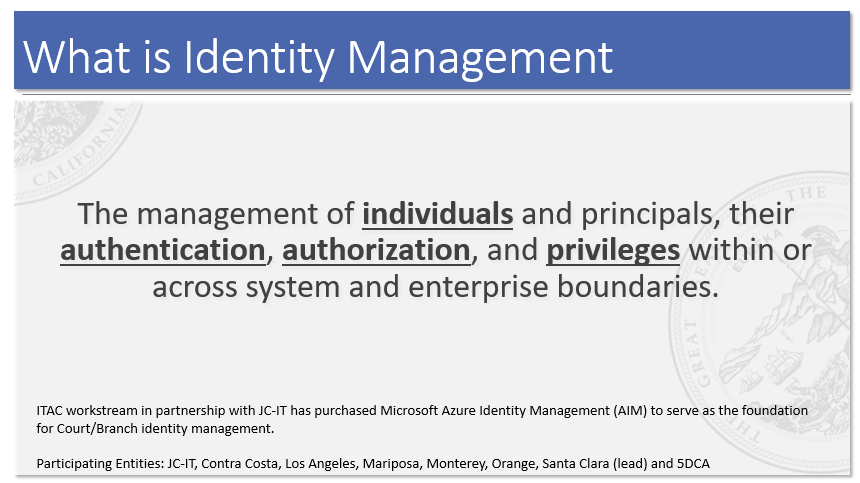
Update to Judicial Council Technology Committee and TCPJ/CEAC.

Snorri Ogata, CIO, Los Angeles Superior Court

This document is meant as a companion document to the PowerPoint of the same name. Please pardon the informality of the writing style!

The Judicial Council has proposed rule changes (SPR18-37) out for comment to “make limited amendments to rules governing public access to electronic trial court records and creates a new set of rules governing remote access to such records by parties, parties’ attorneys, court-appointed persons, authorized persons working in a legal organization or qualified legal services project, and government entities.” Foundational to these rule changes is the notion of Identity Management.

This companion document attempts to clarify the role of Identity Management in support of the proposed Rule Changes, educate the reader on the technical workings of Identity Management and outline how Identity Management extends beyond the presenting opportunity of enabling privileged remote access to case information.



Slide 3 – Identity Management Definition

Identity Management in the context of the Court and case access involves individuals being authenticated, authorized and granted extended privileges to case access services offered by the Court, the Branch or an external Service Providers.

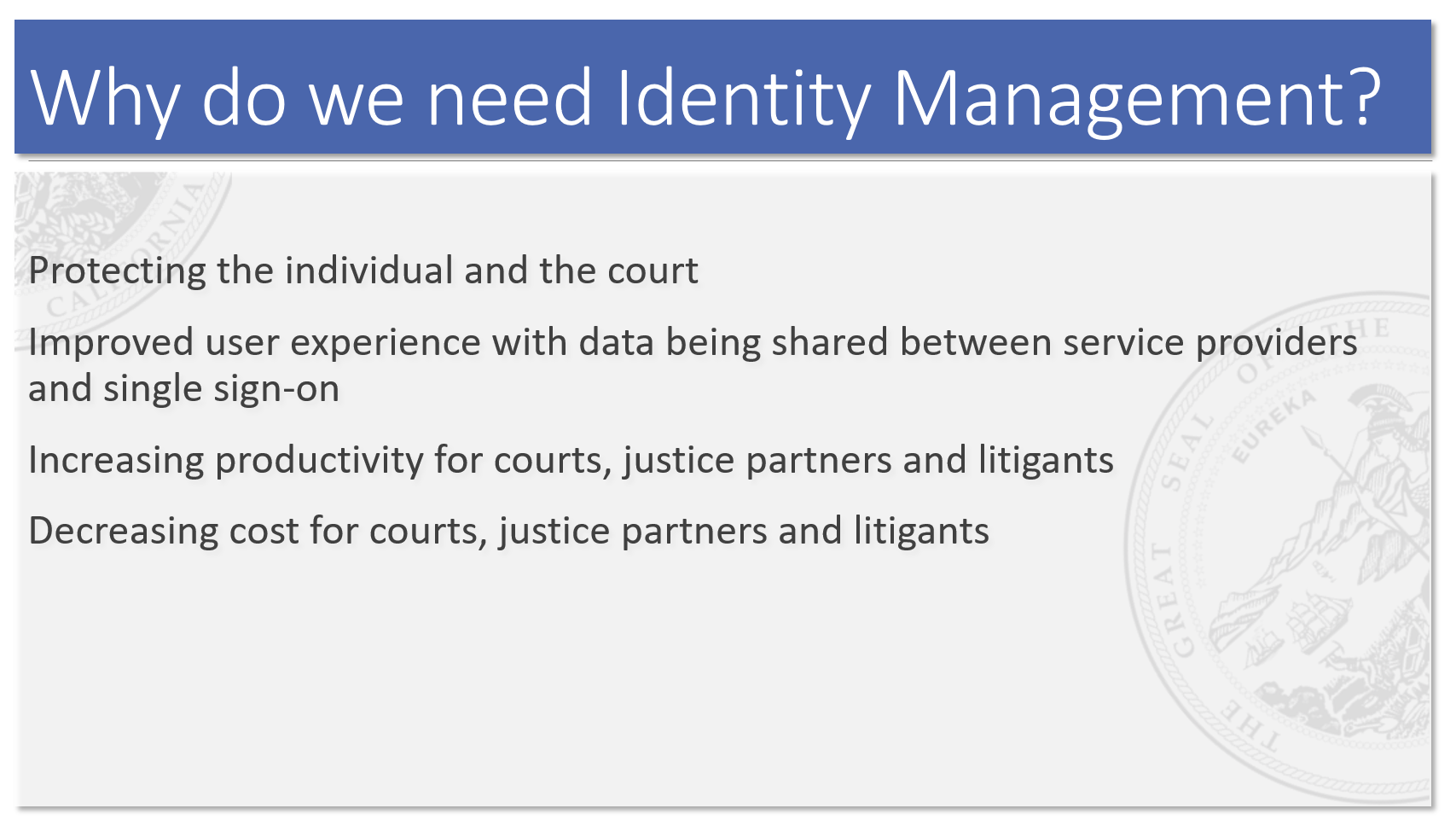
From an information technology perspective, foundational to the proposed rules and Identity Management is the notion of a claim. In answering the question “what individuals have a reasonable right to the extended benefits of remote case access?” the system must know several things (attributes) about the individual. Some example claims and attributes that are implicit in the proposed rule changes include:

* A **party** to an action or proceeding. Their claim to remote access is that it is their case.
* An **attorney of a party** has at least two parts/attributes to their claim. First, the individual is an attorney. Second, the attorney has a defined relationship with a party for a given case.
* A **court appointed person** (to a case) has a claim that their role in the case is ordered by the Court, but the duration of their claim for remote case access may be temporary or restricted.
* **Authorized persons working in a … government entity** is an individual who’s claim to remote access is based on his/her active affiliation with a government agency and that agencies need to interact with the case or cases in a given litigation area.

This paper attempts to describe why and how Identity Management is foundational to not only privileged remote access to electronic case records but how it can be foundation to many other digital court services as well.

**Why do we need Identity Management?**

For simplicity we will presume that the non-public individuals and entities covered in the proposed Rule changes have a reasonable need and/or justification for remote access. The challenge then becomes how to identify these privileged users, how to substantiate their claim to privileged access and how to protect the information being accessed.



Slide 4 – Benefits of Identity Management

As slide 4 highlights there are several benefits to Identity Management. First and foremost is about privacy. Protecting the individual and the Court from sensitive information being inappropriately shared. In the physical world we manage this through the principle of practical obscurity by making people come to the courthouse to view case information. Once at the courthouse, if the information is deemed sensitive, the Court may take the added step of having the individual validate their identity (show driver’s license) to see the sensitive portions of the case file.

As the Courts continue their journey toward digitization the human interaction at the courthouse to protect information become outdated especially when the case “file” is no longer a physical case record. The person is now typically redirected to a computer that provides electronic access to the case. For sensitive information they may be provided a PIN that grants temporary access to viewing the case record.

Likewise, in cases involving justice partners (e.g., District Attorney, Child Welfare) who frequently interact with the physical case file at the Court (or in the courtroom), the elimination of the physical case file requires the Court to create new methods for electronic sharing. Directing these individuals to public hallways with public access terminals is not efficient so the Court (and partners) need to craft new access solutions.

Once these access solutions are built for courthouse access, why not grant these individuals with a privileged claim to case information the ability to view the information when away from the Court? Remote access increases productivity for courts, justice partners and litigants. Case information is just a click away.

Remote access also reduces costs for all involved. Fewer people at the courthouse to view records frees up resources for other value add services. Parties and partners can have extended windows of access that may be more convenient which further drives down costs of traveling while increasing their experience.

Finally, an authenticated and authorized individual can access an array of digital services through a single, common identity. An SRL can create their on-line identity when working in a self-help workshop. That identity (and some information) can then be carried forward to document assembly tools that complete Judicial Council forms. Their identity can then be carried forward to e-filing and ultimately privileged case management once the case is active. This notion of a single authenticated and authorized identity improves the user experience.

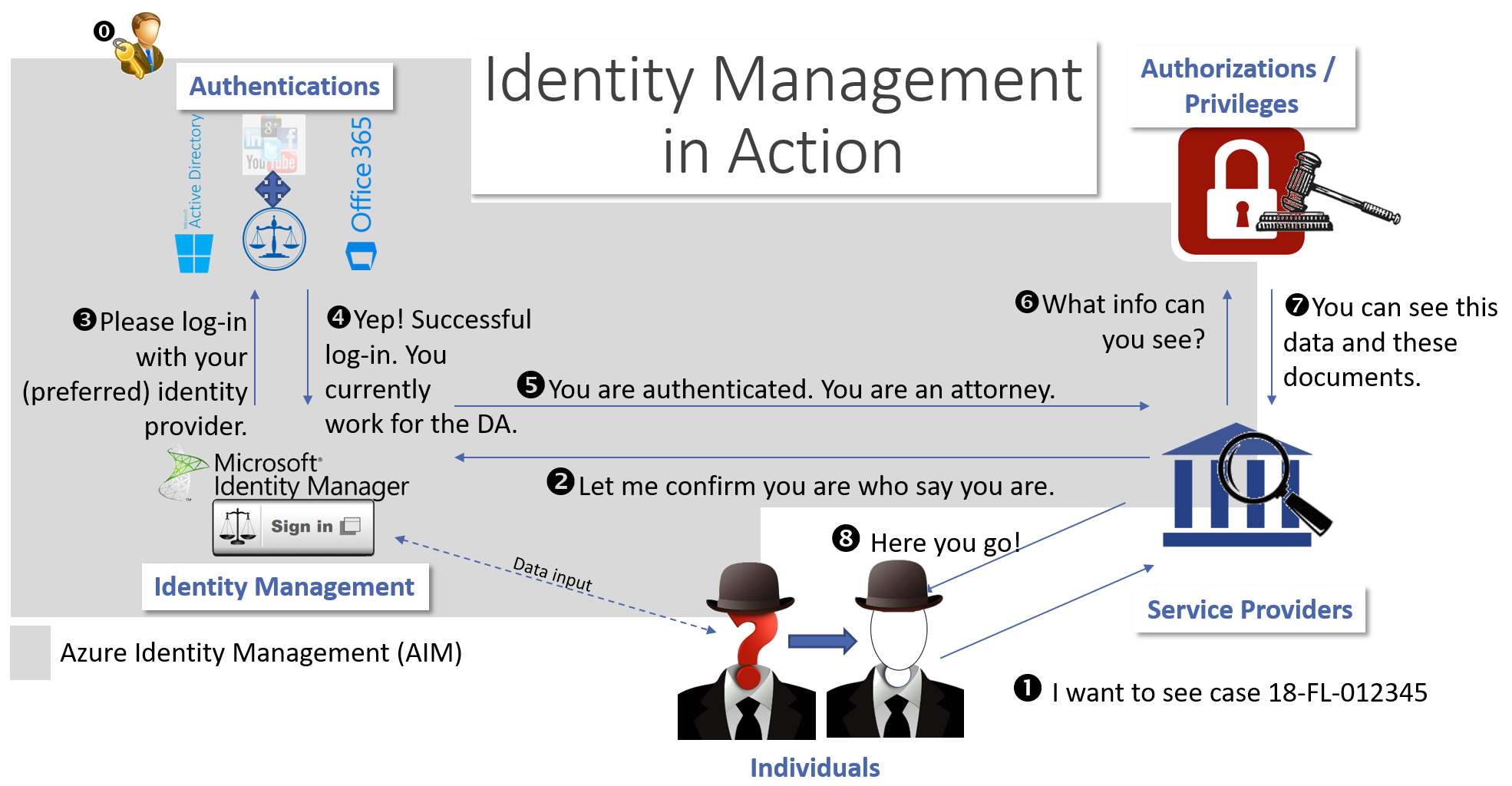
Identity Management protects the Court, makes everyone more efficient and increases our customer’s experience when interacting with the digital court.

**Deconstructing Identity Management**

While Identity Management might seem daunting (slide 5 illustrates that point!) it is also technology that is well understood and widely used today.

Some examples of Identity Management in your day to day life include:

* Using your Facebook account to complete a restaurant reservation on Open Table
* Doing mobile banking from your phone
* Buying products from Amazon from multiple platforms
* Allowing Quicken to download your bank transactions to help manage your household budget
* Remotely accessing your email
* Many, many more



Slide 5 – Identity Management in Action

In the digital world identity is the key and the glue to unlocking protected services and connecting together an individual’s identity across multiple services that they trust. As the Courts complete the first steps of our digital journey by upgrading our case management systems, we must take the next steps to ensure our investments are enablers and not barriers to doing the business of the Court. Identity is at the center of most transactions.

There are four primary components to Identity Management:

**Service Providers** are the starting point. These web applications provide services that the individual wants to consume/use. It could be e-filing or privileged access to case information or any number of other services. The key is that many services require some knowledge of who you are. Identity Management helps orchestrate the process and pass along information to other components/services to ensure the security of the transaction.

**Identity** is the next step. Does the person requesting a service have the necessary credentials? The Identity Management system proper serves two primary roles:

* Facilitate the registration process and capture information about the user that helps substantiate their identity (and optionally share information between service providers) in future interactions
* Orchestrate the authentication/authorization process for Service Providers

A key step in registration is deciding (if appropriate) how your identity will be authenticated at all future interactions with service providers.

**Authentications** can be handled by social sites (e.g., Linked In, Google, Facebook) or organization sites (e.g., Office 365, federated Active Directory) or by the Identity Management system itself. Authentication handles the process of validating the individual making a request for services has an on-line identity that has been validated with an ID and password created during the registration process. While Identity Management systems can use a number of external solutions (e.g., Facebook, LinkedIn, Twitter) to handle ID and password authentication, the preliminary recommendation is that for external users (litigants, private attorneys) their identity and password should be tied to the judicial branch identity solution and not to a social media solution. The simplified thinking here is that the Courts are more like a bank (that makes you create a bank-specific identity) than we are like Open Table (which allows you to use Facebook to authenticate your identity when making a reservation).

Justice partners, however, can and should authenticate through Active Directory (the underpinning of Office 365, the selected Identity Management solution and in use by every governmental entity). This added layer of integration allows the justice partner to assume the accountability for managing access to services.

**Authorization / Privileges** is the next step. In the case of remote case access, the authorization step validates the claim:

* Is this person a party to the case?
* Is this person appointed to the case?
* Is this person an employee of an authorized governmental agency?

Collectively these underlying technologies help service providers validate a user’s claim to privileged capabilities. This, however, is only part of the capability. The other part is driven by the individual trial court as illustrated in the Los Angeles Justice Partner Portal.

**Los Angeles Innovation Grant**

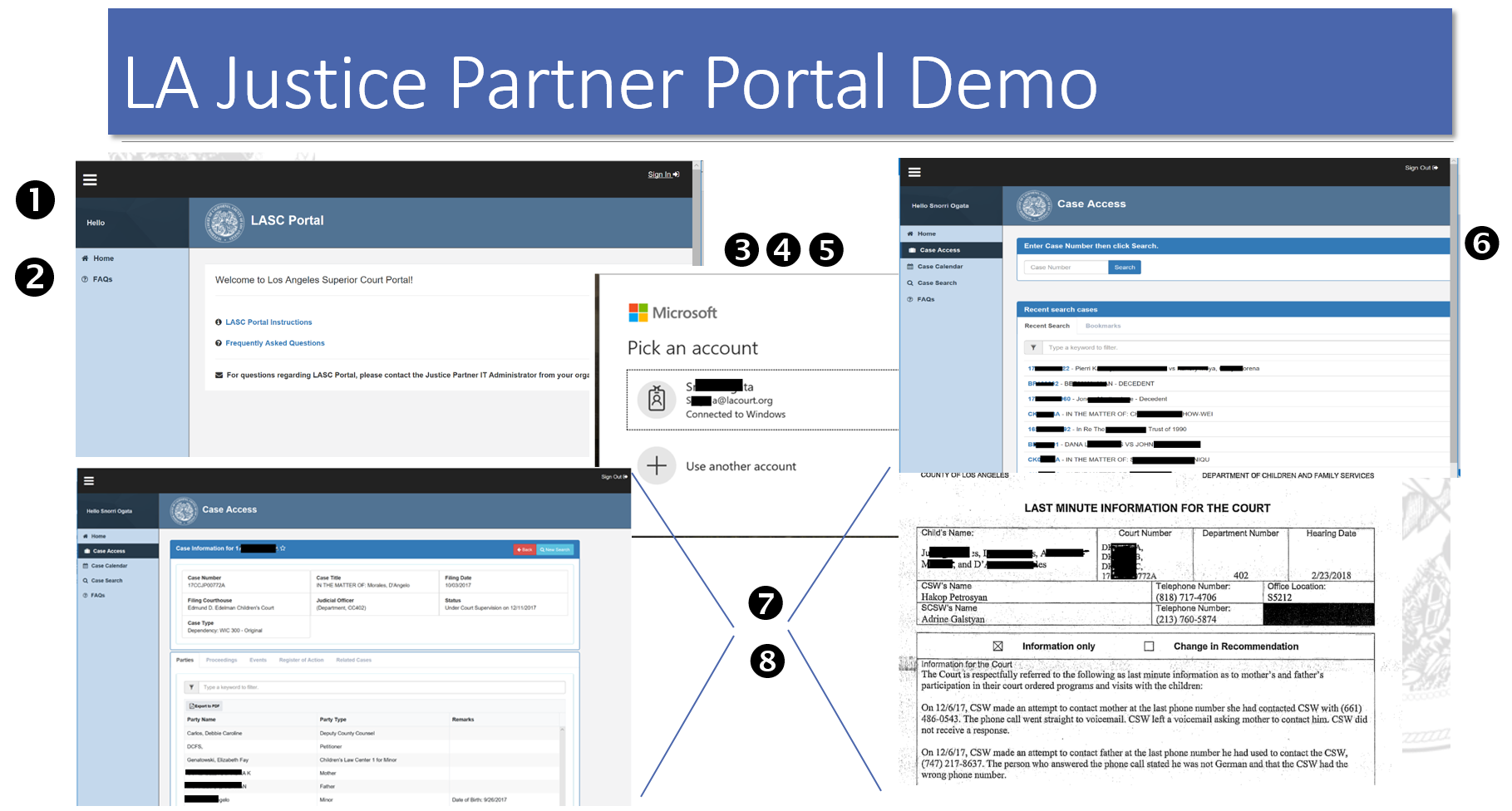
The Los Angeles Superior Court (LASC) has a privileged case access system that has been operational since September 2017 built upon the same technology selected by the ITAC Identity Management workstream. The Justice Partner Portal (JPP) allows privileged users to remotely view case data and documents in Juvenile Dependency, Family Law and Probation. Other litigation areas are scheduled to come on-line as the Court completes its Case Management System upgrades.

Before the portal was launched to the justice partners, however, LASC needed to establish the non-technical foundations such as:

* Establishing an MOU that governs the use of the system and the responsibilities of the partner in protecting information
* Determining which organizations have a reasonable claim and could/should be granted access
* Determining what case data and documents will be shared and if different roles in a given organization should see different information
* Creation of Active Director (AD) tokens that enforces the information sharing rule (e.g., attorneys at the District Attorney can see documents while non attorneys at the DA’s office can only see calendars).

Once those foundations are in place the Justice Partner (after signing the MOU) designates a technology administration resource in their organization to administer these tokens for their employees. While this sounds complicated to the non-technical audience, this is a commonplace activity in every Information Technology Department. This is done through a common “group management” process within Active Directory (AD) which is the Identity Management system used by almost every organization to manage user identities and access rights within their organization.

The Agency AD administrator needs to add the token to each employee who is being granted privileged access (this is step 0 in the slide 5). The MOU likewise points out that the Agency is responsible to remove the token when individuals change jobs and to remove employees from their AD system in a timely manner when they terminate employment. Fortunately, these are all common processes in every technology department in every organization. The average time to “train” an organization for their portion of identity administration with the judicial branch identity solution, including infrastructure set up, is thirty (30) minutes!



Slide 6 – Los Angeles Superior Court Justice Partner Portal

Slide 6 illustrates how JPP leverages the Identity Management technology by highlighting which numbered step from Slide 5 (Identity Management in Action) is being executed when the user is remotely accessing case records.

1. The user (let’s say an attorney that works in the District Attorney’s office) goes to the Court Justice Partner Portal.
2. The system asks them to sign-in before being granted any access.
3. Based on the user’s profile, the action of signing-in is redirected to an authentication service provider. In this case Microsoft Office 365 which the DA’s office uses for email.
4. The user signs in to JPP using their agency Office 365 credentials! If successful, Microsoft passes back to the Identity Management System (and eventually to JPP) a token that was assigned to the DA when access to JPP was established (step 0 in slide 5)
5. The Identity Management system then informs JPP that:
   1. The user that registered…
   2. Has authenticated with their identity provider (in the case of justice partners we enforce the use of Microsoft O365 in Los Angeles County)…
   3. Is an active employee (e.g., still has the ability to access systems at the DA’s office)…
   4. Has a Court defined access token associated with his User ID that recognizes his role as an Attorney
6. JPP then validates that the token is recognized and consistent with the organization (e.g., protecting against another organization trying to access case information pretending to be an attorney at the DA’s office).
7. JPP then passes the case data and documents that are consistent with the user’s claim, and
8. Securely presents the information to the user in a web browser

While it sounds complicated with many moving parts, the identity management technology is quite mature and quite inexpensive. In fact, for many use cases the services are already owned and paid for by the respective organizations (Court and justice partner).

The proposed rule changes also introduce three concepts/features that are not fully dealt with in this introductory presentation but should briefly covered. These are identity proofing, delegated access and auditability.

**Identity Proofing** is the process by which a physical person is associated with his/her digital identity. This can be done electronically or in person and typically involves an external authority (e.g., passport or driver’s license) or service (e.g., e-filing proves/validates case access for a given case). Some examples of identity proofing:

Justice Partners: In the case of justice partners the assumption is that the federated AD credentials (step #4) and the security token (step #0 and 5) sufficiently identify that individual’s proof of identity relative to their case access claim.

Attorneys: Upon registration, an attorney’s identity must be validated by the email address registered with the state bar. The registration system sends an email to the address registered with the State Bar to complete the registration process. Once confirmed, the attorney (as identified by the bar number and email address) is considered proven.

E-Filer: For an SRL that e-files on a case, the action of e-filing followed by an acceptance by the e-filing clerk, completes that transaction and proves the identity (provided the same email address is used for e-filing and identity registration). If you successfully file on a case, the email address used (and registered with the EFSP) is deemed to “verify” that person’s identity for that case.

Non e-filing Litigant: A litigant that wants to examine their dissolution documents may need to come to the Court to complete the verification process. This may involve showing a form of government identification and being provided a PIN that will bind the individual to a case. We are still architecting this piece so more to come.

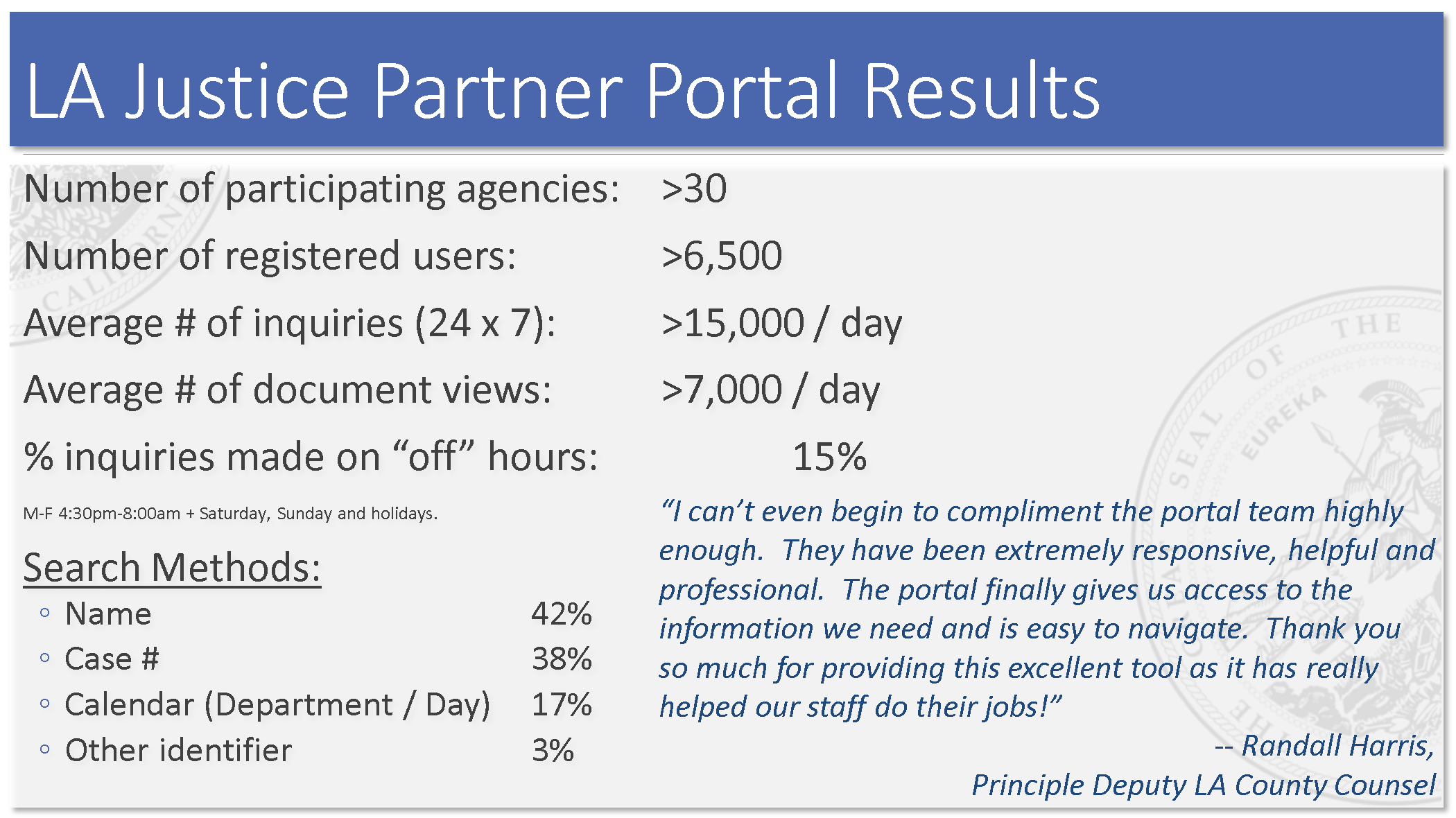
**Delegated Access** is a specialized use case of Identity Management. The principle is simple. An individual who has been “identity proofed” and has privileged access can, on their own authority, delegate their access claim to anyone they want. A litigant could grant access to their case to a friend or relative. An attorney could grant access on their behalf to a case in which they are associated to their paralegal or associate.

The action of delegation carries with it the accountability of appropriate use. Should the relative or paralegal be found to have inappropriately shared case information inconsistent with the terms of use, the delegating individual is accountable. The auditability function (below) provides visibility on case viewing activities by an individual and their delegate(s). The delegator can also revoke delegated access at any time.

The ease in which delegation could be technically implemented plus the built in auditability makes delegated access a superior alternative to what would almost certainly happen otherwise. It was anticipated that individuals would simply share their ID/password credentials with others to facilitate information sharing and that reduced the Court’s (and individual’s) security position.

**Auditability** is the recording of every action in the case access portal. To ensure the highest level of accountability, all access to case information controlled through a user’s claim will be recorded in audit logs. These logs shall be examined periodically by the MOU organization (if applicable) to ensure appropriateness of use. The LA Portal has a built in Agency Manager to assist the agency (and the court) monitor who is using the system and what cases are being explored. This also provides the Court with the ability to quickly and easily provide measures of success as shown below.

**The Los Angeles Justice Partner Portal Results**



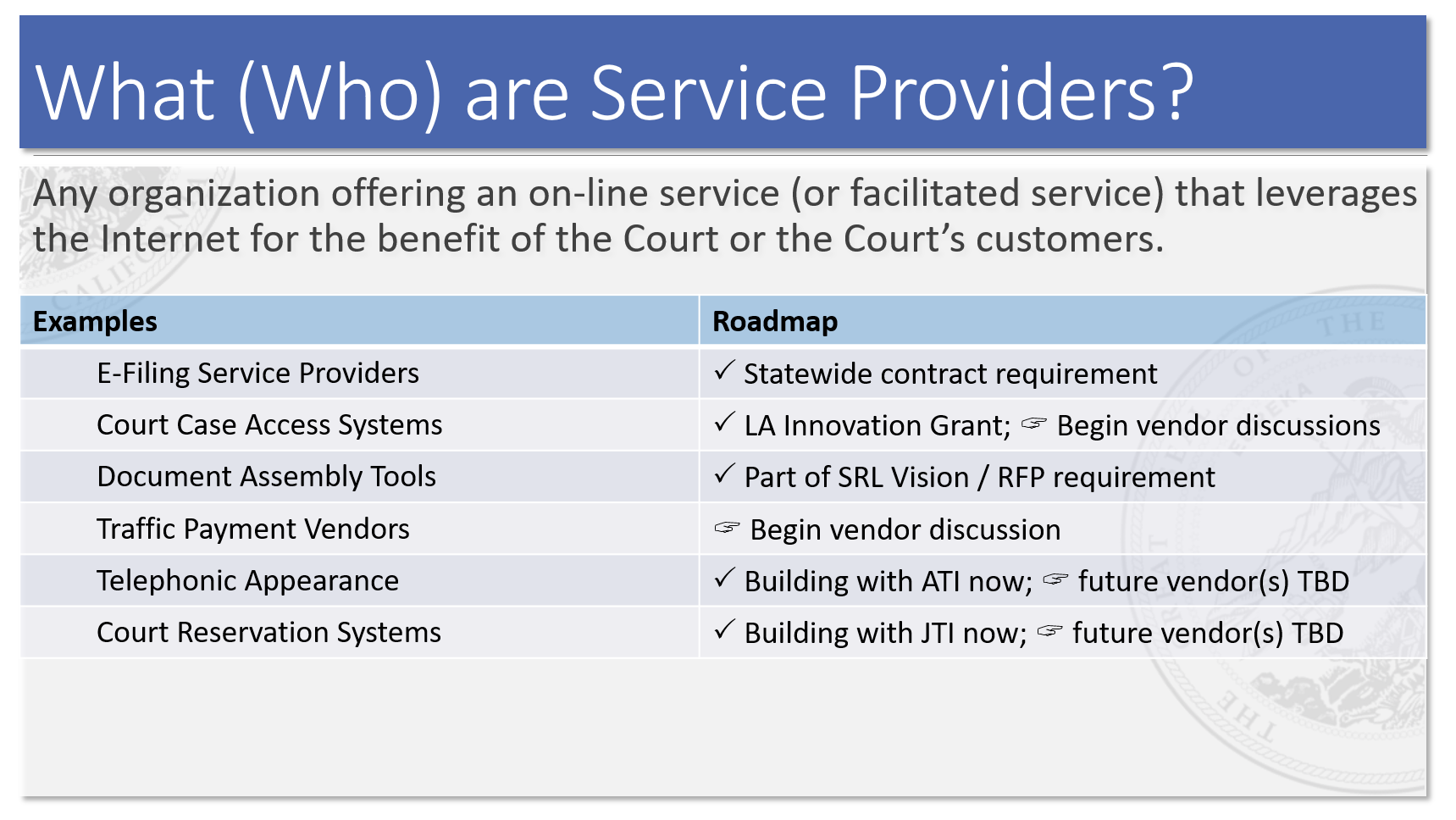
Slide 7 – LASC Results

The LA Portal has been in use since September 2017. As slide 7 highlights as of September 1st the portal is used by over 6,500 employees at over 30 justice and/or authorized partners (e.g., Probation, Child Welfare, CASA) who access Juvenile Dependency, Probate, Family Law and Traffic case information 15,000 times a day!

They access cases based on name searches, case number searches and calendar searches. Los Angeles County also has other identifiers that are often associated with a child or case than can be used as well. An exciting statistic is that approximately 15% of all case inquiries occur when the courthouse is not open which was not possible before when we only had paper files. That is improved access!

**Service Providers and Roadmaps**

Although the bulk of this paper has focused on Identity Management in the context of privileged case access, Identity Management has many other uses. Slide 8 highlights known examples of “service providers” that exist today to support the digital court.



Slide 8 – Service Providers

A service provider is an organization offering an on-line service that leverages the Internet for the benefit of the Court or the Court’s customers. All of these service providers exist in one or more CA trial court today:

* E-Filing Service Providers
* Court Case Access Systems
* Document Assembly Tools
* Traffic Payment Vendors
* Telephonic Appearance scheduling and management
* Court reservation systems

All of these service providers can benefit from a single Identity Management system.

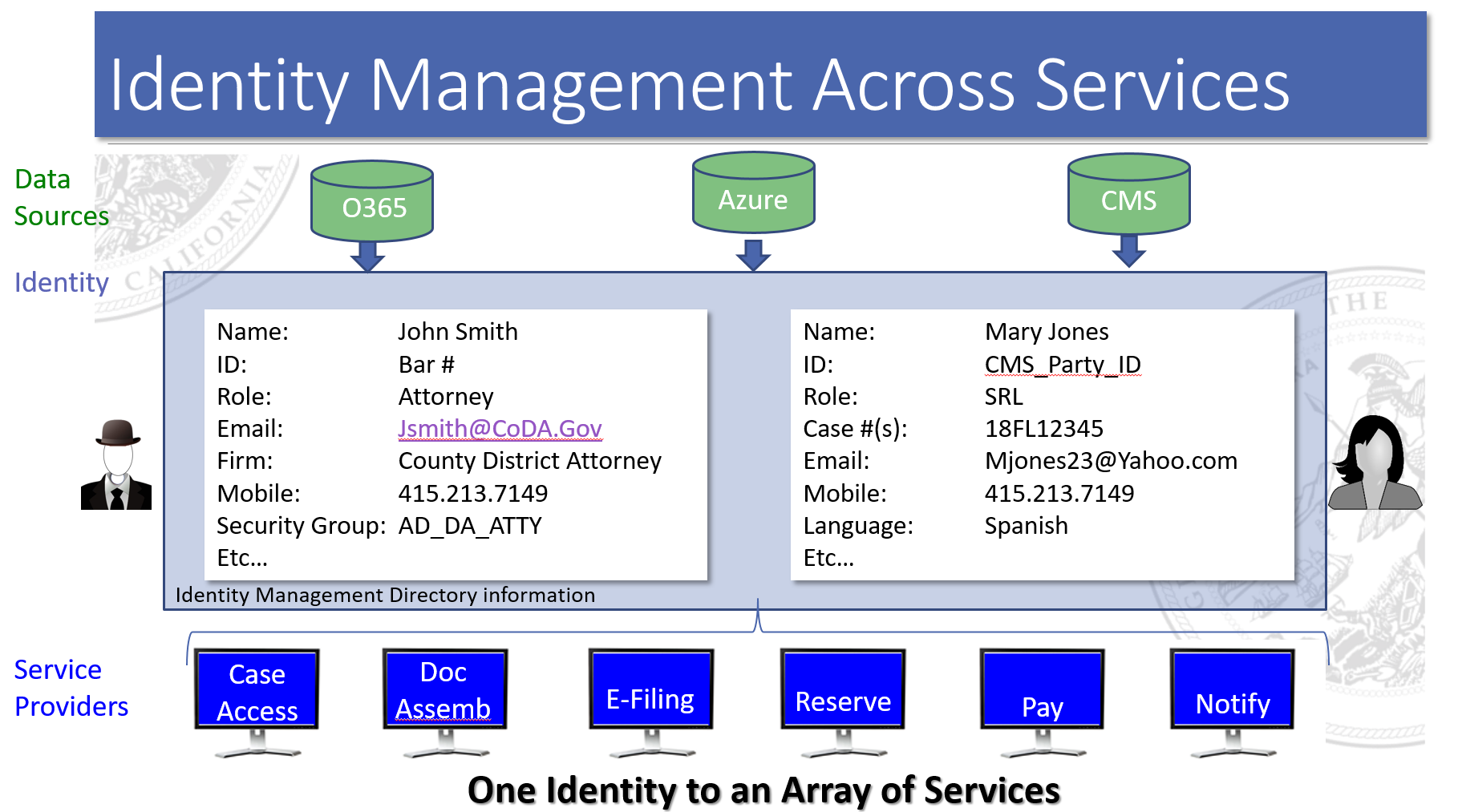
In fact, the statewide e-filing procurement anticipated a branch-wide identity solution and listed it as a core requirement. The simplifying assumption was that a person who e-filed (through one of dozens of e-filing service providers) should be able to use their same identity credentials to access a case or schedule a telephonic appearance.

An SRL who used a document assembly service to complete Judicial Council forms through a plain language interview should be able to use that same identity to e-file on a case and access their case remotely after filing.

These are all examples of “single sign-on”. One identity to access multiple systems (or services).

**Identity Management Across Services**

Slide 9 attempts to illustrate another benefit branch-wide Identity Management. The notion of authorized information sharing across service providers.



Slide 9 – Identity Management Across Services

As a user takes advantage of additional services, more information can be gathered (e.g., mobile phone number or language need) and securely stored in the identity management system. As the user takes advantage of other service providers they will have the option of sharing specific data elements to lessen duplicate data entry which improves overall accuracy.

Imagine an SRL who created an identity to do document assembly. In the registration process, document assembly wants to know if the user has a preferred language. Mary indicates Spanish. Mary quickly realizes that filing a case is more complicated than completing a form (or three) so she uses the Self-Help Reservation System to schedule a slot at an upcoming dissolution workshop at the Court. The scheduling system automatically sees that Mary’s preferred language is Spanish so by default it shows workshops that are taught in Spanish. During the workshop registration process Mary is asked to (voluntarily) provide her mobile phone number so the Court can send her a text message reminder about her upcoming appointment (which will be done in Spanish). Later, Mary wants to subscribe to the “Notification” service to get a text message anytime there is an action on her case or to remind her of upcoming hearings. The Notification service knows Mary, her language preference and her mobile phone number without asking. Mary’s identity facilitates improved services.

**Next Steps**

The Identity Management workstream AND the Los Angeles Innovation Grant Portal are at the beginning stages of a new way of providing on-line services. Much work is left to be done.

The initial phase of the ITAC Identity Management workstream was focused on evaluation and selection of the best Identity Management technology solution. Extensive research was done on the various solutions available but Microsoft’s offering were the only offering to be identified in every ranking list (e.g., Gartner, Forrester and others) that also satisfied federal security standards. It was also one of the least expensive solutions because many courts already own parts of the licenses.

The initial Portal work done by Los Angeles has demonstrated that the technology is affordable and can be implemented. The Innovation grant calls for Los Angeles, in collaboration with several other courts (Monterey, Orange, Santa Clara to name a few) to develop a roadmap and playbook to help other courts embrace the technology.

Both initiatives (along with the proposed Rule of Court changes on extended remote access) are now ready to tackle the more nuanced policy questions, such as:

* Should individuals be allowed to choose social providers (e.g., Facebook) to be the authentication source for their identity when interacting with branch services?
* What restrictions on case data and documents should be put into place to refine access (and restrictions) for various litigation types? For example, can a justice partner search using a date of birth field?
* How to educate and empower the user to decide which data fields associated with their identity are sharable with other service providers? Does a ‘payment service’ need to know that Mary speaks Spanish?
* How to educate and empower the user to delegate access to their claim?

There are many policy questions that need to be refined as we gain more experience with the new digital court. A key next step is to cast a wider net to work through these broader, non-technical questions.

**Identity and Access Management Q&A**

Is there a plan for individuals to create a “judicial branch” user account?

Yes. The notion of the judicial branch user account (aka judicial branch identity management, or JBIM) was introduced in the statewide e-filing procurement and has been carried forward and incorporated into various innovation grant projects.

If yes:

* Where is this in the planning stages?

The plan is to introduce JBIM as each new “service provider” comes on line with a requirement to use the JBIM solution. The statewide e-filing vendors will be required to do this but I don’t expect them to be compliant for many months (especially since the contracts still aren’t signed!) or even a year or two. Los Angeles received an innovation grant to create an identity management capability for e-filing and another grant to build a statewide Index and Privileged Access portal capability leveraging JBIM.

The first grant is effectively complete which coincided with the work of the ITAC Identity Management workstream. Microsoft Azure Identity Management was selected as the underlying technology for JBIM. This technology was fully utilized in the second grant as an advanced proof of concept.

Los Angeles is also working with ATI (a telephonic appearance vendor) right now to change their identity management to use the JBIM solution. That work is progressing well for a launch date in the fall of 2018.

Finally, preliminary discussions with Journal Technologies are underway since JTI is the Civil CMS and Civil E-Filing vendor for Los Angeles.

All other services will need to be planned and road-mapped including notification to the vendor community for inclusion in their on-line services.

* Has a unique identifier been selected?

It is an email address. The Microsoft solution allows the user to choose with Justice Partners being the notable exception.

There are actually two products under the hood of JBIM. The “B2B” (business to business) solution basically connects the branch identity to the justice partner’s Active Directory environment. For justice partners using Office 365 this connection is automatic. For everyone else there is a small integration effort to “federate” their Active Directory with the JBIM solution. It sounds more complicated than it is. It takes about 30 minutes to setup..

For non-justice partner users we use the “B2C” (business to consumer) solution. The user registers (provides demographic data like name, email, bar#, …) in the JBIM solution. Out of the box the Microsoft solution supports the JBIM proper to be the authenticating authority (e.g., where ID and password are validated, similar to a bank) or to integrate with social providers (like Facebook, similar to Open Table) to handle the ID/Password authentication step. At this time we are recommending that JBIM controls the log-in experience because the Court is “more like a bank than a restaurant”.

* Will this account verify the individual’s identity?  Or will people be able to create whatever account they want under any name they want?

For partners the verification will be managed by the partner’s active directory. In the case of the LA Innovation Grant portal you need more than a login account to gain access. The agency’s identity management person (typically a network administrator who updates the internal Active Directory) has to ALSO create and associate “AD Group” (provided by the Court) to unlock certain feature. This two-step process (has an active account with the justice partner AND has the AD Group token added to their user profile) confirms their identity. The “name” associated with their activity is the name associated with their Agency’s Active Directory.

For attorneys (a variant on the B2C solution) the current PROPOSAL in the LA grant is that the attorney registers with the solution, creates the JBIM ID (email) and password, and provides their Bar #. The registration process then reaches out to the State Bar and sends an email to the address that the state bar associates with that bar #. The attorney then will need to go to that email system and confirm their intent to register. Once they complete that process, their identity is deemed verified. They will be able to use whatever name they want.

For everyone else, the “identity proofing” step needs to be defined in the context of the SERVICE PROVIDER. For example….

* If someone is paying a traffic ticket, we presume them to be themselves for that ticket. No identity proofing required. Just give us the money!
* If someone is e-filing (SRL), the action of e-filing followed by an acceptance by the e-filing clerk, completes that transaction and the identity (provided the same email address is used for e-filing as registration) completes the process. If you successfully file on a case, the email address used (and registered with the EFSP) is deemed to “verify” that person’s identity for that case.
  + NOTE: A policy question that needs to be examined is whether the accepted e-filing action then automatically verifies their identity with any/every other case that they have with the Court? Both Tyler and Journal have a notion of a unique party identifier, so once the party is validated on one case does that validate you on all other related cases? This will be examined by the ITAC workstream.
* Finally, in the worst case, an individual might need to come to the Court to complete the verification process. This will involve showing a form of government identification and being provided a PIN that will bind the individual to a case. We are still architecting this piece so more to come.
  + NOTE: There are 3rd party services that verify an identity (e.g., “which of the following 4 addresses did you NOT live at?”) but they cost money and we still haven’t determine how viable these methods are at this time. This will be examined by the ITAC workstream
* Will those e-filing be required to use this user account?

Yes. It was a requirement of the statewide e-filing manager RFP.

* Are the EFMs building this in?

They will be. It was a requirement of the statewide e-filing procurement and is part of the contract.

* Is there a plan for attorneys and law offices to create “judicial branch” user accounts?

Sorta. It can be handled under the “delegated access” capabilities or we could explore federating their Active Directory. Another policy question.

If yes:

* + Has a plan been identified for “attorney” versus “firm” access? For example, Attorney A at Firm A is the attorney, but then Attorney A leaves Firm A, Firm A keeps the case.

This is a good use case that will need to be unpacked. In Los Angeles attorneys on cases are tracked at the Attorney level. In Orange, they are tracked at the firm level.

Assuming the Court and CMS tracks things at the attorney level, then the bar number is the glue. Service Providers like the LA Case Access Portal will do an “authorization” step. Attorney John Smith, Bar # 123456 has a registered account (created and verified in 2017 with the state bar and confirmed in 2018). John tries to access case 17-CI-987654 and the Access Portal makes a further inquiry into the CMS to verify that John is still the ACTIVE attorney of record. If the answer is yes, they John gets to see the case. If the answer is No, he is presented with an error message that he is not authorized to access this case.

* + So does the Firm have access or the attorney?

We have not worked through the mechanics of the Court/CMS tracking at the FIRM level vs the Attorney level, so I don’t want to over-represent what we can do. This will need to be explored further with the ITAC workstream and several courts.

That said, the “delegated access” feature allows a person previously ‘verified’ to access a case the ability to delegate access to others based solely on their authority. Implicit (and explicit) in this action is accountability. If they grant access to a delegate, they are liable for its use.

The Policy decision that will need to be worked through is whether delegated access is handled on a case-by-case basis (makes sense for SRLs) or on an account by account basis (probably makes more sense for the paralegal to be granted access to all of Attorney John Smith’s cases).

The LA Innovation grant calls for us to work out the technical and policy details and then present a roadmap to courts and service providers (including CMS vendors) on how to implement. That is due next year but my hope is that 5-7 courts will already be using the system by then.

* + What about when they want notice to go a paralegal too?  Can they set that up?  Or is it one email to one person?

Notice would likely be covered by the “Notice” service provider (!) which is distinct and separate from the e-filing service provider (EFSP) and the case access service provider and the Reservation provider and the Payment provider. However, an EFSP could make this extended noticing a differentiating aspect of their e-filing service and they could manage this. This sounds bureaucratic but it’s FUNDAMENTAL to the component architecture. Each component (or service) CAN stand on its own and/or CAN be stitched together to create a new end to end service. For example, Case Access and Notice could be put together for alerts on cases in which you are a verified party.

So… how would Notice work? Users could sign up for the Notice service using their branch ID. They would then “subscribe” to the cases they want to follow. When an event/action happens in the CMS the Notice Service (possibly for a fee!) would send communications out to anyone that is subscribed to that notice.

But… notices can also come from the Court CMS (courtesy notices, notice of judicial assignment change) or from the EFSP (your e-filing was accepted) or other Service Providers.

Bottom line is that “notices” would be a function of a service provider which is distinct from an identity management solution (although most certainly related!).

* + Is there a plan for organizations to have “judicial branch” user accounts?

Yes, but… Justice Partner organization can federate their organization accounts with JBIM.

* The proposed access rules would give broad access to certain legal aid organizations.  Is it contemplated that these organizations would have a “judicial branch” account?

The architecture is SUPER flexible and does not presuppose a judicial branch account in the fullest sense. Identity Management in the context of the Court involves individuals being authenticated, authorized and granted extended privileges. The foundation behind extended privileges is a “claim”. A claim is the set of attributes that determines the level of privilege a user receives.  The user claim can be validated by a number of attributes:

* Case Affiliation. Is the party affiliated to the case as an individual (e.g., SRL, attorney) or organizationally (justice partner)
* Case or Organizational Role. Is the party’s role defined at case level only (e.g., SRL) or is their access broader (e.g., attorney with multiple cases, justice partners, …).
* Active Association with case and/or affiliation. Is the attorney still the active attorney? Is the attorney still a member of the bar? Is the attorney still employed by the DA?
* Identity Proofing (verification of identity). Is their claim further validated by an external means (e.g., attorney validated by the CA Bar, justice partner validated by an Access Group token, SRL validated identity and PIN)
* Delegation . Is the user granted access on behalf of a valid claimant (e.g., paralegal granted access by attorney of record; individual granted access by SRL/party)?

The ability to understand an individual’s relationship to a court-related service (e.g., case access. E-filing, reservations, payments) protects the individual and the Court from inappropriate information sharing.

Before the “claim” kicks in, the user has to be authenticated. All users must REGISTER with the branch identity solution and the can choose one of 3 (generally) ways to authenticate as described above:

* Their organization identity (e.g., B2B use cases)
* The branch identity (which will be their email address)
* A social account of their choosing (not recommended)

So… yes. It is anticipated that everyone using privileged court services will have an account registered with the branch identity solution through an MOU (and federated active directory or an individual account).

* If yes, would authentication be happening at the JC level?  Or would each court have to authenticate?

See incredibly long worded answer above! But a HUGE goal in all of this was to lessen the load on the Court for identity administration. User administration is managed by the user (or their organization).

* Assuming all of the above are yes, to what extend have case management system vendors been engaged so they can plan for linking to these accounts?

Through the Innovation Grant Los Angeles is building the “connectors” to Tyler Odyssey and Journal eCourt and defining the necessary interfaces to support this “fine grained” access approach for others. Most of the interfaces exist out of the box for the CMS vendors so we anticipate only doing a little tweaking to support other vendors.

For vendor provided portals, the vendors will need to be notified to modify their solution to be compliant by some future date.

* Assuming all of the above are no….then are ideas being developed on how each court could afford the remote access rules being proposed? (This one is a little unfair.)

That’s the hope of the Innovation grant. Our grant was to build a framework for a statewide index (a very thin veneer of case information that CRCs require Courts to make electronic) supplemented by a distributed architecture that allows individual courts to:

* Host all access (index, plus case detail and documents) in the statewide repository (think Microsoft Azure cloud), or
* Host all Index data centrally and host all case detail and documents locally
* Something in between (e.g., Orange, Monterey and Santa Clara all seem to be leaning toward a hybrid third case because they have software engineers)

The key, however, is that as we move from Index (largely public) to “privileged” access each court will need to determine their tolerance for information sharing. The proposed CRCs provide more air cover than what currently exist. The Portal as built will have a number of recommended configurations (e.g., LEAs get to see CDLs and DOBs but County HR departments do not for traffic citations) but access can be controlled at a very fine grained level (down to specific data elements and specific documents). The more control that an individual court wants the more local configuration will be required.

That said…. I really think we’ve have this figured out. The “lead courts” on the LA grant (LA + the 3 above plus Contra Costa) and JC-IT have been working on this for almost 2 years now. And, Los Angeles has version 1.0 in use today by 3,531 users at 13 justice partners who access Probate, Family and Juvenile Dependency case information 15,000 times a day!

**Glossary of Terms**

Active Directory Group - a software construct that allows the management of multiple individuals (i.e. employees) within a common category. Groups are often used to define roles or other affinities. They simplify access control. A group, for example, might be all juvenile social workers at the County child welfare agency or all attorneys working for the district attorney.

Affiliation - specifies a person's relationship to an organization or case in broad categories. An organization affiliation could be an employee of the district attorney’s office. An individual affiliation could be a litigant or an attorney on a case.

Agency Manager – a feature of the Justice Partner Portal that allows privileged users to monitor active users and usage of the portal by employees granted an Active Directory Group role in the Agency’s Active Directory environment. The Agency Manager draws on the Audit Trail to track and report usage of JPP by individuals within an Agency.

Authorization - an extra security step that allows or denies access privileges to a solution provider’s services (e.g., application, data or documents). When a user signs in, authorization is usually performed before authentication (see "Authentication").

Audit trail – a system that traces detailed transactions related to a system or service. An example is access to a case record will record the date, time, user identity, case number and action that was performed in a case access portal.

Claim – a set of identifying attributes that assert an individual’s right to see case information.

Claim Attributes – specific pieces of information that taken together substantiate a user’s claim. Sample claim attributes include: affiliation with the case or organization, active association with the case or organization, has a defined role through an Active Directory Group, is appointed to a case by a judge.

Federation - an agreement between identity providers and service providers that allows for the sharing of information. It lets users of a service sign on to said service through one single identity provider. For example, Office 365 allows users to sign into different websites using their Office 365 credentials. Other examples include Facebook Connect , Google (Gmail), Microsoft (Hotmail), Linked In, etc.

Identity Proofing - the process by which a physical person is associated with his/her digital identity. This can be done electronically or in person and typically involves an external authority (e.g., passport or driver’s license).

Multi-factor authentication (MFA) – While not mentioned MFA is an optional additional security requirement that requires the use of at least two different methods to verify a user's identity (most commonly a password along with a card/PIN, authentication token, or one-time password sent via SMS).

Privilege - an additional construct that governs access management. Privileges allow certain individuals to have extended capabilities. These privileges usually come from and are maintained through the evaluation of entitlements and application access policies. An example of a privilege would be an Agency’s network administrator who has the ability to set up and change what an individual is authorized to access.

Service Provider – an organization that provides clients with services. Examples include organizations that provide on-line resources to help individuals: e-file on a case, remotely access a case, make an appointment with the self-help center, make a payment with the Court. A service provider is expected to manage its relationship with the branch identity provider and trust its capabilities to manage policies required to operate the service responsibly.

Single-factor authentication uses a password or other single method to verify a user’s identity.

Single Sign-on Authentication, or SSO - a service model in which users log into one single platform that gives them automatic log-in access to multiple applications for a certain period of time. Users using this system only have to remember one set of credentials, as opposed to learning a new password for each application.