eDirectory as Core Service

Johnnie Odom
The School District of Escambia County (ECSD)
Technology Transfer Partners (TTP)
June 2022

eDirectory Capabilities

- Limitless data modeling.
- Enormously scalable (lots of data and fast).
- Replication and Partitioning that is flexible and “just works”.
- Natively stores data as objects and properties/attributes.
    - The same data could be organized in tabular form, but NOSQL databases have shown that this paradigm is not one-size-fits-all.
- Multiple types of relationships (Hierarchical, Linked, Membership/Grouping, Search by Type or Value).
- Strong type and consistency enforcement.
- Changes to schema supported as foundational feature.
- Multiplatform.
- Strong support from vendor.
- Well-understood backup, support, and troubleshooting.

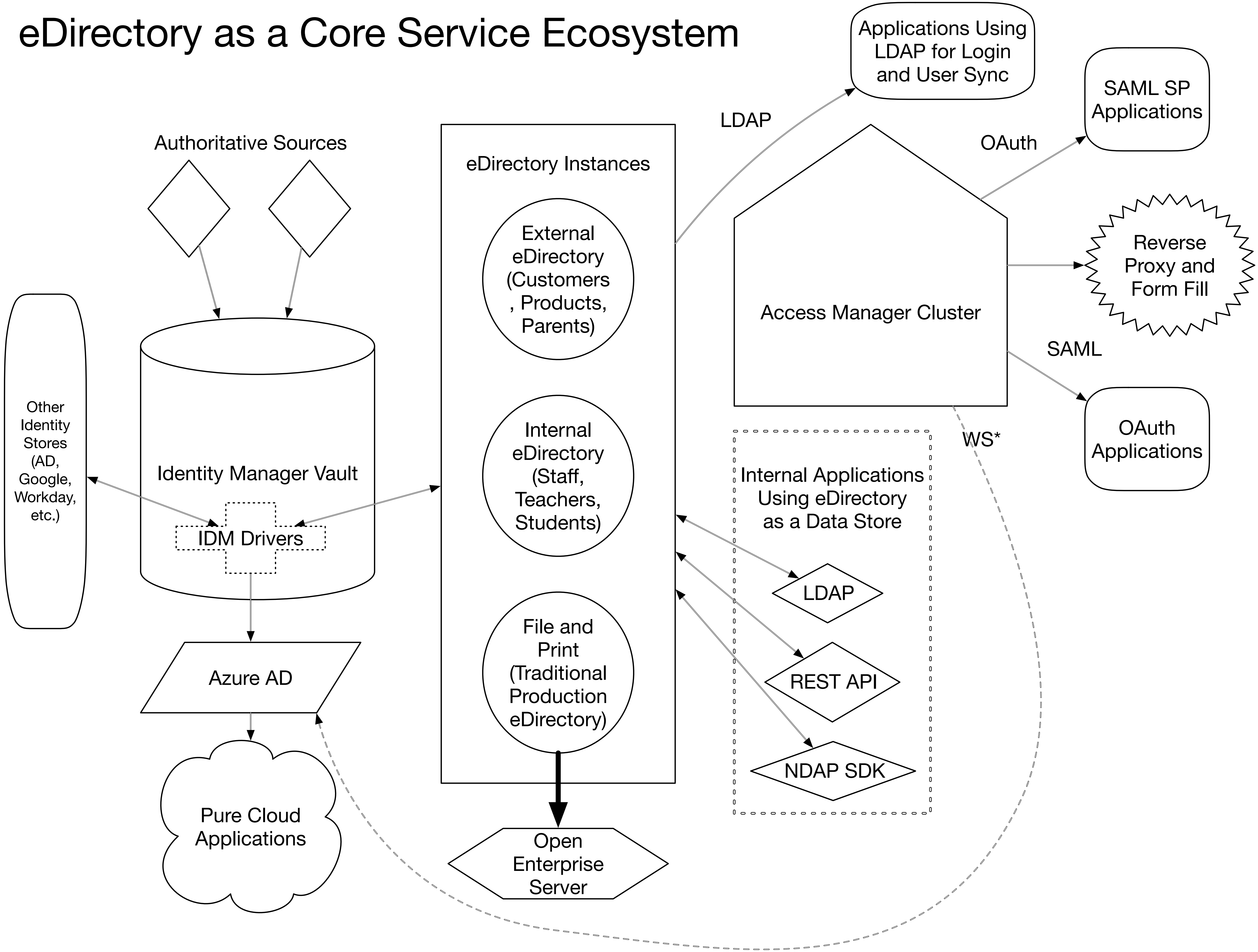
Identity is Valuable

- If it were not, Google and Facebook would not be spending billions on free services to acquire identity information.
- Identity can be a series of facts about a person.
- It can also be what the person is in relation to someone else or in a specific context.
  - Martin Buber's "I and Thou" if you want to get deep.
  - Or the "child, parent, spouse, worker, congregant, consumer" roles of every day life.
- When people come together to work in concert or as part of a system, the expression of their identities is part of the whole as well as being an individual element.
  - When the group of people is large enough, it moves to "Enterprise" scale.
- Because expression of identity is so important to an organization, it is important that the electronic systems built for that organization reflect the full model and desired capabilities of the organization.
  - Therefore, those systems which are most important, must reflect the real structure of the organization, or which have other systems derive from them are also those systems which must be most flexible and under the direct control of the organization.
  - Yes, I am going to suggest eDirectory does this best.
    - Certainly for on-Prem, Cloud is still a question.

Services in a Cloudy World

- IT Skillsets getting more difficult to train because the middle career stage between “frontline service desk” and “backend engineer” is being hollowed out.
- Users interact with interfaces, largely written in JavaScript or a thin layer of native application GUI.
- Actual work done by ever-more complex systems protected from direct intervention
  - Containers, data centers, etc.
- This has also happened with eDirectory
  - Direct login to eDirectory (a la Novell Client) is no longer the case and services are indirect too.
  - Subsequently, eDirectory is less visible but more important similar to other services.
    - We can forget how important it is.

eDirectory as a Core Service Ecosystem



Accessing eDirectory Data For Use

- Directly:
  - NDAP - More complete but older and used mainly by legacy systems.
  - LDAP - More universal but limited unless extended.
  - REST API - New, but a shim to LDAP.
- Indirectly:
  - OAuth via Access Manager - Can send JSON formatted user information with transformations.
  - SAML, WS*, etc. via Access Manager - Fit for specific purposes.
  - IDM Drivers - Can be expressed in any manner (SOAP, text, proprietary) but requires that a driver exists and may only be useful for endpoint system.

Systems Using eDirectory as Application Data Store

- Access Manager
  - All configuration information stored in eDirectory
  - Why? — Replication!
- Open Enterprise Server
  - Inheriting the “store everything in the Directory” approach of NetWare
  - They have attempted to move away, but the core remains
- iPrint Appliance
  - Legacy from OES but it still works
- Identity Manager
  - For the Vault, to act as a hub and superset of all identity data

Identity Manager

- Projects identity information to other systems using a standard workflow.
  - Standardization means that process can be preserved and business logic codified when working with disparate systems.
  - Every identity system believes it is the most important, but few of them allow organizations to work exactly how they would like.
    - Therefore we populate all of them and let them believe that they are “the boss”.
      - Exception is Azure AD which can be very powerful in a Cloud context, but still lacks eDirectory’s flexibility.
- Identity Market has largely settled on simple data copies, no one is building a true competitor.
- Challenge is recognizing that Identity Management is a core function of the organization and training personnel to use IDM.
  - Compiling data in the Vault from authoritative sources is useful.
  - Standardizing workflows is good for process and business logic.
  - Projecting to any and all identity-aware systems automatically is the big win.

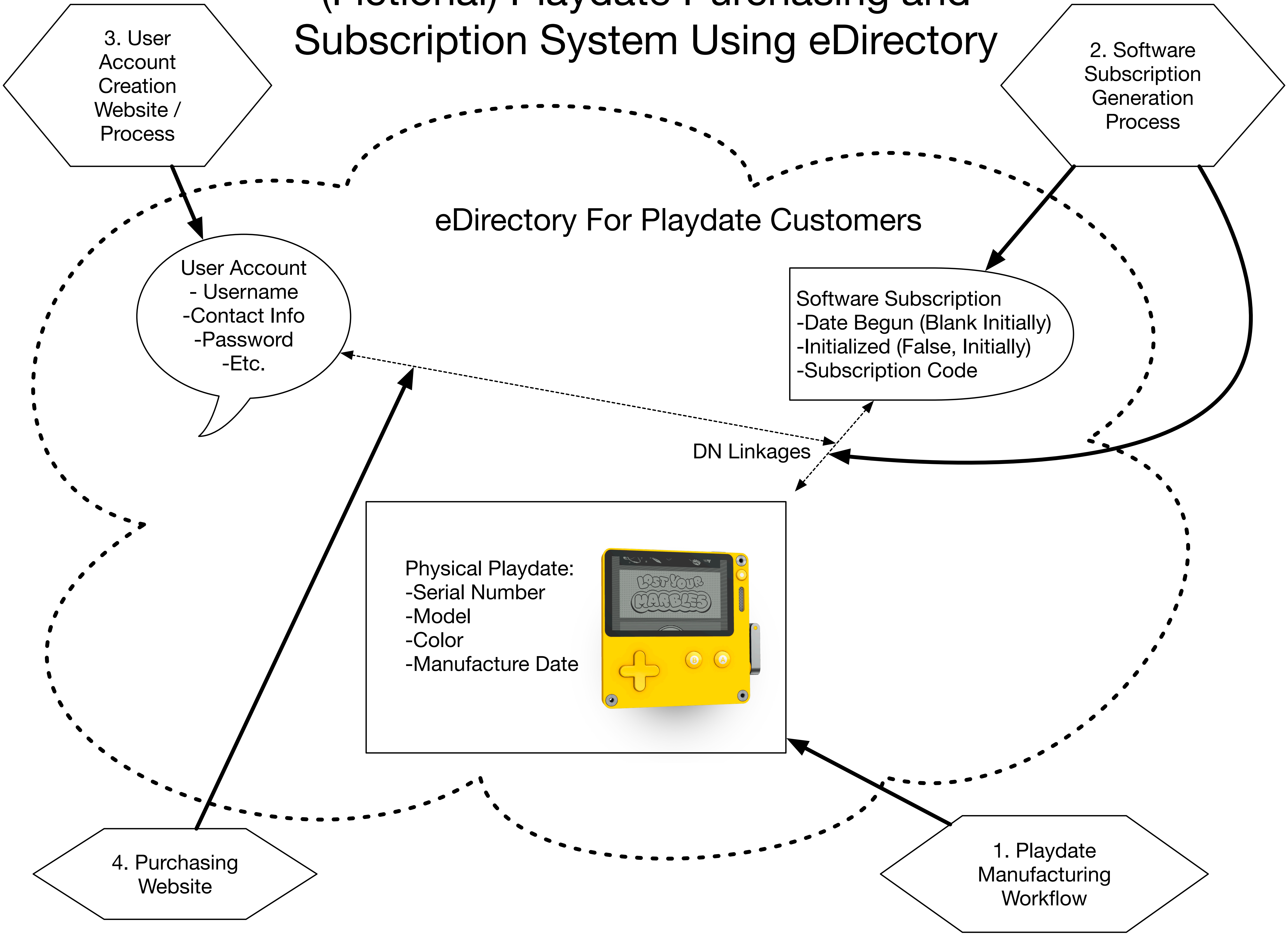
Access Manager

- Three uses: Reverse Proxy, Federation, and OAuth
- Reverse Proxy
  - Original usage of product.
  - Handles form fill
  - Handles transformations.
- Federation
  - Bread-and-Butter use — SAML and WS*
  - Extremely useful for secure login to many, many services.
- OAuth
  - Capability with the most potential.
  - Allows secure and complex transfer of per-user information to any application, especially internal.

eDirectory as Internal Application Store

- Simple usage via OAuth and Access Manager.
- Or can be used a la Access Manager for configuration data.
- But what if we leverage the model?
  - The company Panic! has a new device called the Playdate (https://panic.com and https://play.date)
  - Playdates are sold out until 2023.
  - Comes with a game “season pass” subscription.
  - What if we used eDirectory to connect users to their hardware and subscription on purchase?

(Fictional) Playdate Purchasing and Subscription System Using eDirectory



Closing Points

- eDirectory has a place as a core service in a wider ecosystem of organizational services.
- It remains the premier on-Prem Directory Service and the movement of the market to the cloud and simpler models means it will not be replaced.
- Challenges
  - The question is not whether an organization embraces eDirectory, but whether it embraces the responsibilities and challenges inherent in using identity information to its fullest.
  - And, related, whether it handles technical challenges head on or settles for “what everyone else does” or “enough to get by”.
  - These challenges may involve eDirectory, but they are not about eDirectory.
- Identity Manager and Access Manager are tremendous extensions to eDirectory’s power and purpose.
  - Schools can get them several ways, including the IDV Value Bundle (recommended).
  - Even simple IDM improves efficiency greatly.
  - NAM is worth the cost for SAML alone, but opens great possibilities for internal programs through OAuth.