Authorization Survey Results & Use Cases – Presentation to Concordia Working Group

Identity and Authorization Services Working Group (IAS-WG)
John Tolbert (Boeing)
Gavin Illingworth (BMO Financial Group)
July, 2010

kantara INITIATIVE™

Agenda

Today we will cover the following topics:

1. Overview of Identity & Access Working Group
2. Results of the AuthZ survey conducted by John Tolbert
3. Review seven sample AuthZ Use Cases we have gathered

Overview of IAS-WG objectives

- Grew from an informal identity group hosted by Burton Group – Kevin Kampman and Anne Thomas Manes
- Chartered in Kantara Dec 2009
- 20 voting and non-voting members to-date
- A primary objective is to develop a logical architecture for AuthZ, similar to the one the original group developed for AuthN

Question Summary

- Survey conducted during January – March 2010
- 22 respondents replied anonymously through the Concordia mailing list

1. To help us understand the context of your answers we'd like to know how many users your organization is authorizing?
2. What are the primary use cases and/or business drivers for authorization?
3. Do you currently have a centralized access management system?
4. What type of access management system do you use?
5. Which access control models are supported by your access management system?
6. What types of factors/assertions/claims are supported by your access management system?
7. Does your access management system provide for policy lifecycle management?
8. Does your access management system provide mechanisms for sharing and/or distribution of policies?
9. Does your access management system support the following protocols (Current/Future)? (check all that apply)
10. With which other types of systems does your access management system integrate? (Current/Future)
11. Rate the following features of an access management system in terms of importance for your deployment:
12. Rate your organization's maturity in its ability to manage its information sufficiently for effective and compliant access control to sensitive data resources.
13. Additional comments regarding access management systems:
14. If you are willing to have a follow up conversation, please provide the following information. We will not use this information for any other purpose and will delete it once the survey is processed.

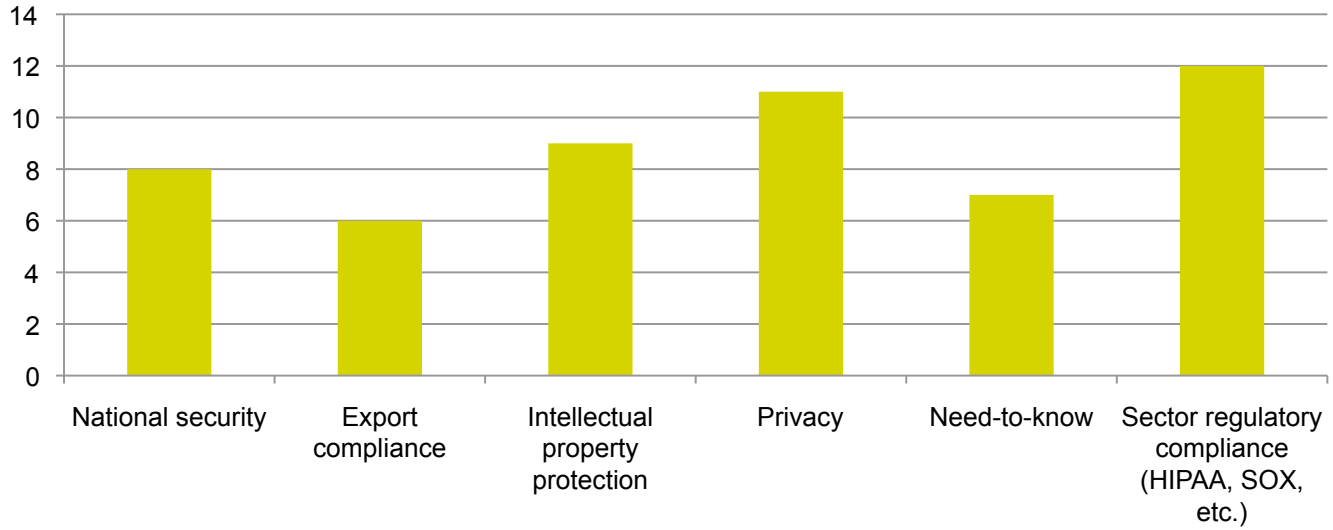
Question 1

1. To help us understand the context of your answers, how many users your organization is authorizing?

	≤100	10+ to 1,000	Thousands	Tens of Thousands	Hundreds of Thousands	Millions
Raw data	~ 100		Thousands	15,000	>100k	1million
	~ 100		6,000	25,000	150,000	1,000,000
			~ 5,000	60,000	200,000	
					500,000	
Total responses	2	-	3	3	4	2

Question 2

2. What are the primary use cases and/or business drivers for authorization?



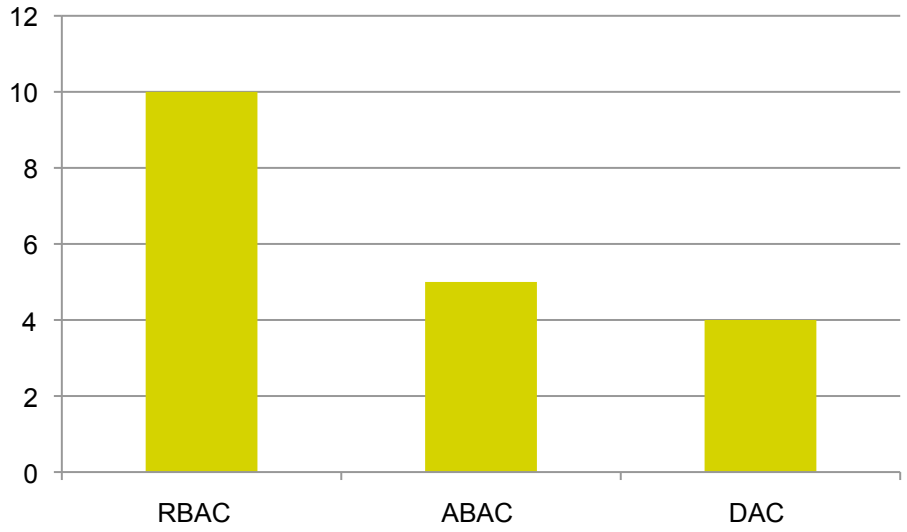
Questions 3 and 4

3. Do you currently have a centralized access management system?
   - Yes = 13
   - No = 8

5. What type of access management system do you use?
   - COTS = 11
   - Custom = 9
   - Decentralized = 10

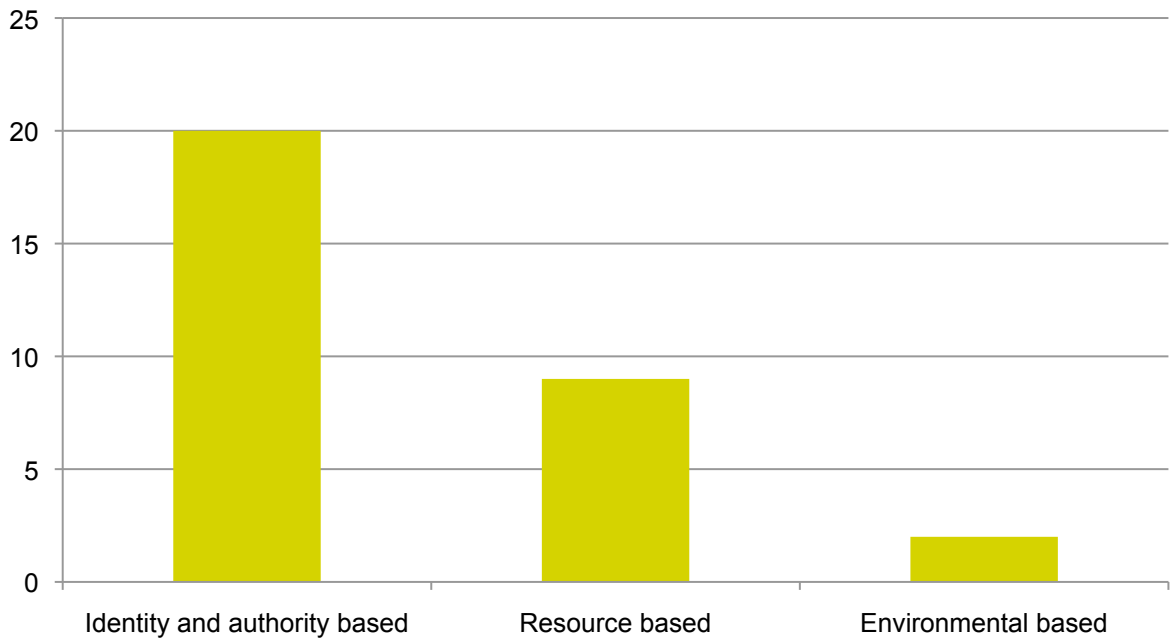
Question 5

5. What type of access management system do you use?



Question 6

6. What types of factors/assertions/claims are supported by your access management system?



Questions 7 and 8

7. Does your access management system provide for policy lifecycle management?

   Yes = 7

   No = 15

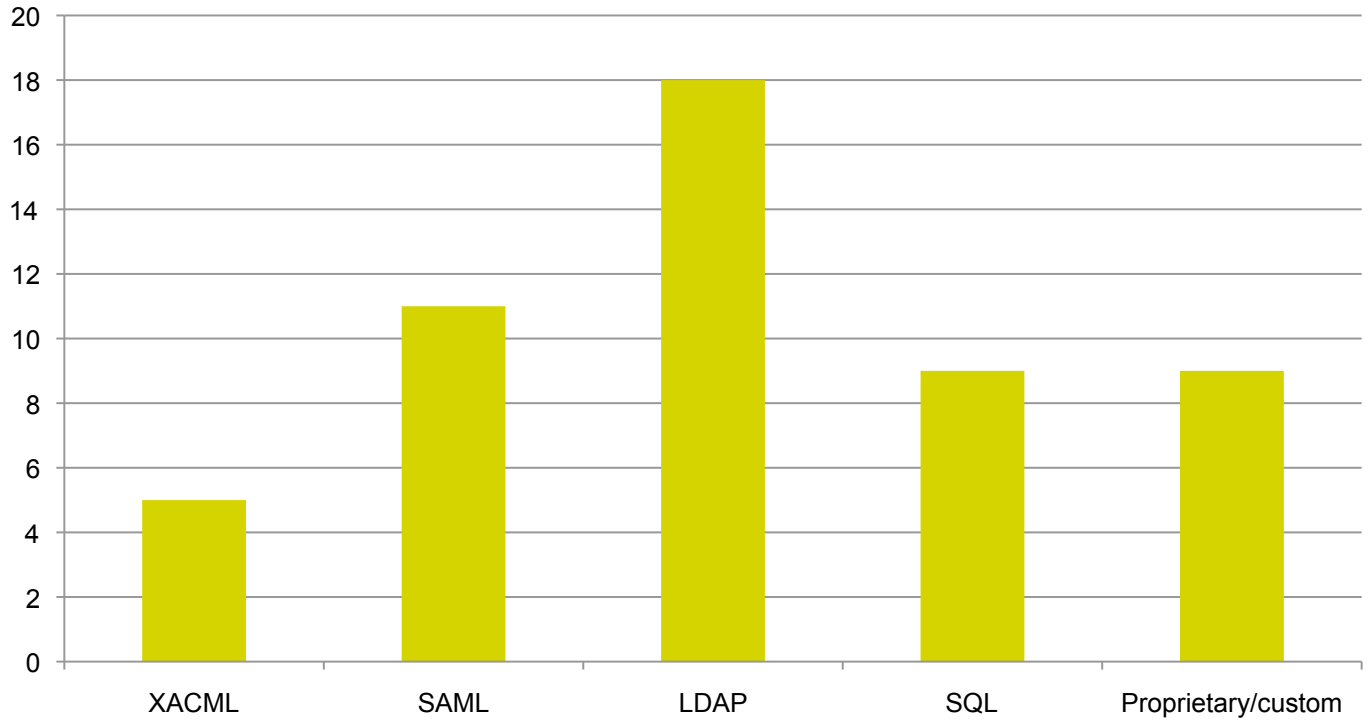
8. Does your access management system provide mechanisms for sharing and/or distribution of policies?

   Yes = 8

   No = 14

Question 9

9. Does your access management system support the following protocols (Current/ Future)? (check all that apply)



Question 10

10. With which other types of systems does your access management system integrate? (Current/ Future)

	Not Important	Slightly Important	Important	Very Important
Performance	0	0	8	12
Scalability	0	0	7	15
Reliability	0	0	4	18
Extensibility to diverse applications and development environments	0	3	7	11
Support for open standards	1	3	6	12
Support for fine-grained authorization	0	7	9	6
Compatibility with legacy systems	2	5	9	6
Ability to mix and match Policy Decision Points and Policy Enforcement Points from different vendors	2	7	8	5
Integration with strong authentication systems	1	5	7	9

Question 11

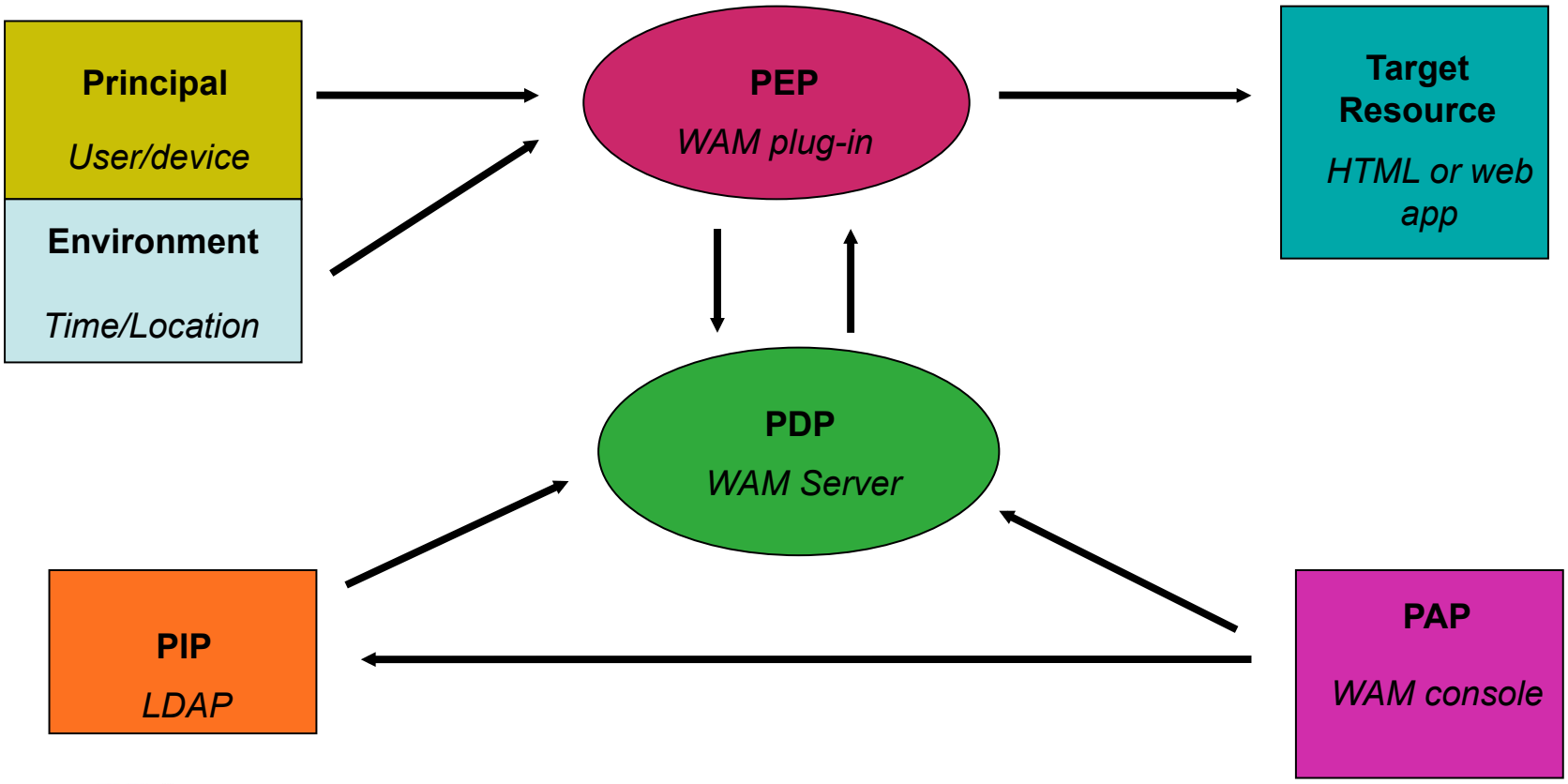
11. Rate the following features of an access management system in terms of importance for your deployment:

	Not required	Very Poor/ Nonexistent	Poor	OK	Good	Very Good
Corporate data model is mature and based on standards where possible	1	4	3	6	1	2
Corporate data model is used effectively	0	4	4	5	3	0
Corporate taxonomy/business rules are mature and cover all regulations and policies for compliance	0	3	7	4	1	1
Corporate taxonomy/business rules are used effectively to categorise data and documents	2	3	3	7	1	0
Corporate document labelling standards exist and include documents owned by other organisations	2	3	1	7	2	0
Corporate document labelling standards are used effectively	2	3	4	5	1	0
Where data is replicated to De-Militarised Zones for external access, data quality and synchronisation management exists to ensure data is fit for purpose	4	1	1	6	2	1
A common authorization rule set exists for all Policy Decision Points (PDP)	1	5	4	3	0	0
Policy Enforcement Points exist at the boundary points for all zones or segregation areas at the network level and within the bus, application layer or database (e.g. vaulting)	2	2	1	8	0	0
Indexes are encrypted and data fields masked or obfuscated to prevent unauthorised disclosure of sensitive information -	0	3	1	8	1	0
Digital Rights Management is used to protect distributed documents and revoke permissions	6	2	2	5	0	0
All permission management and authorisation decisions are audited and permanently recorded	0	1	4	9	1	0

Survey Conclusions

- Reliability, scalability, performance, extensibility, and support for standards are critical.
- Most respondents do not consider themselves very mature in the authorization space.
- More use of centralized authorization systems reported than anticipated.

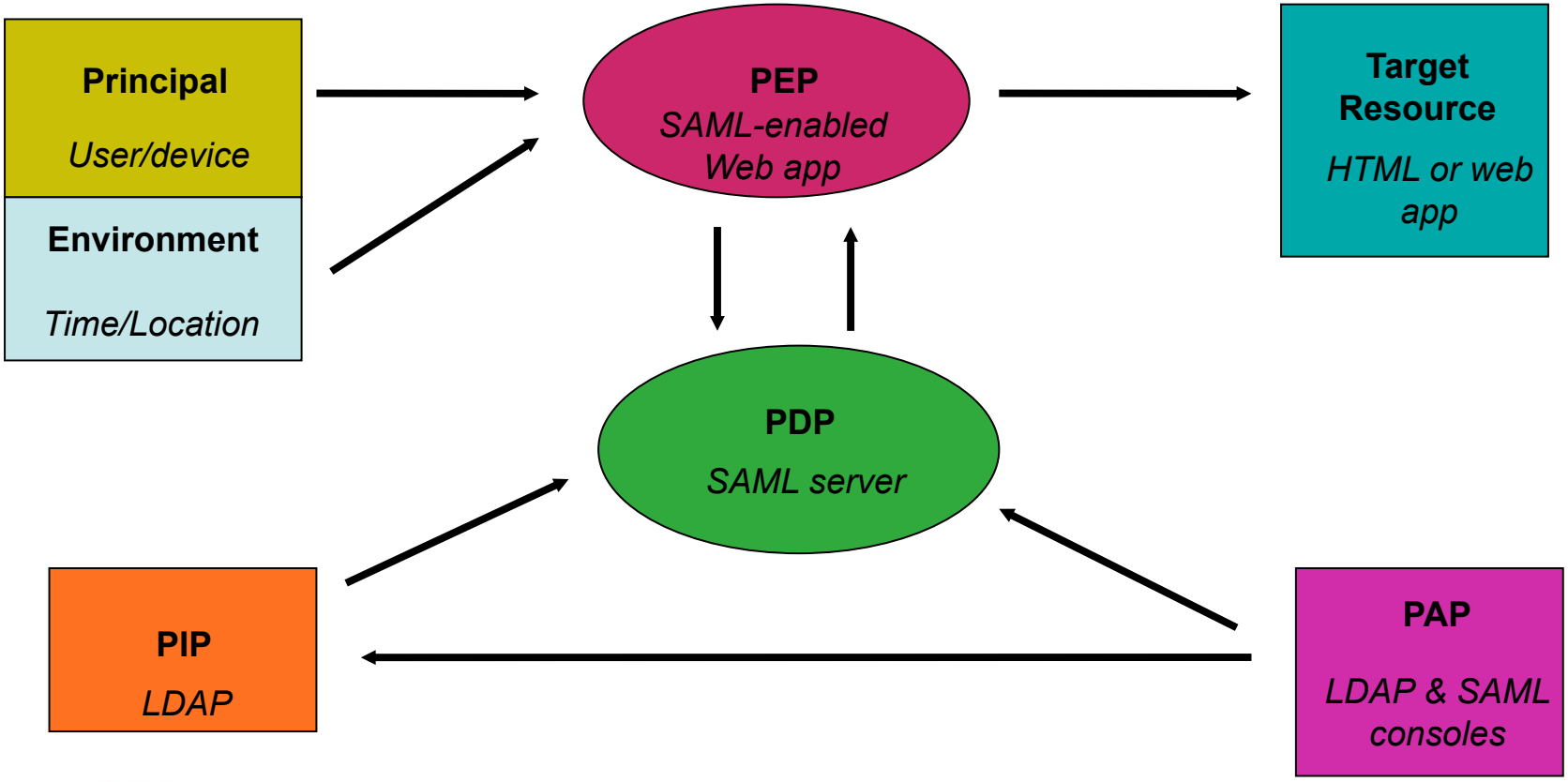
AuthZ Use Case 1 - Web SSO via Web Access Management (WAM) System



Use case details – Web SSO via Web Access Management (WAM) System

Author:	John Tolbert
Brief Description:	Human user requesting access to an html document protected by a web access management system (WAM). Policy information stored in LDAP, authored within WAM.
Goal:	Human user gains access to authorized document or application.
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	User clicks link to protected resource
Steps or flow:	User clicks link to protected html resource; WAM plug-in on host system asks PDP if the user can get access; PDP relies on pre-authored LDAP policy data; PDP returns result to PEP, host system delivers document to user.
Post-conditions:	Transaction logged.
Non-functional requirements:	
Business rules:	Optional rules to consider include regulations (export, HIPAA, SOx), privacy, intellectual property controls, national security, need-to-know, etc.
Issues:	PEP and PDP deployments in this case are limited to platforms served by the WAM agent and server.

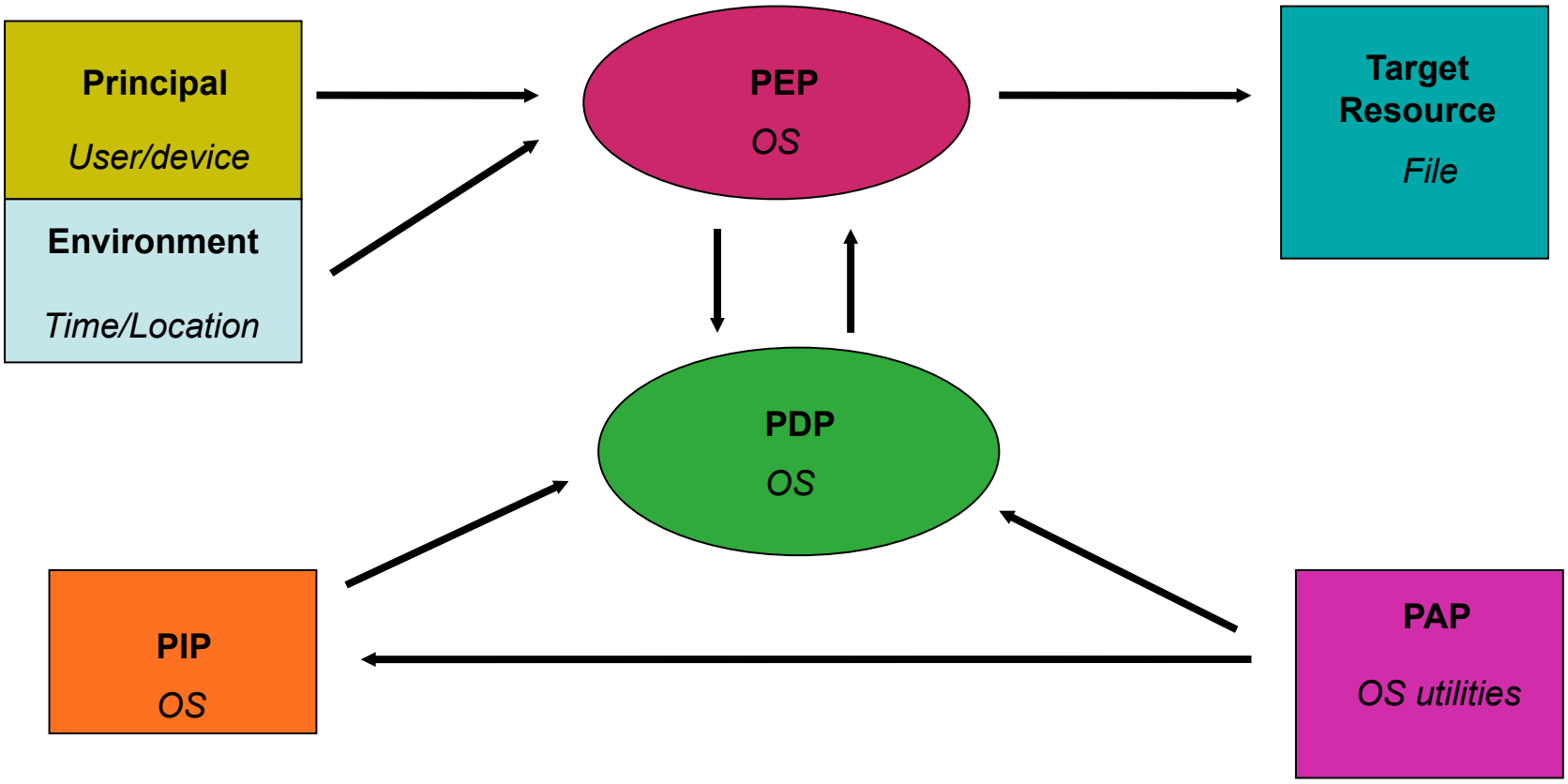
AuthZ Use Case 2 - Web SSO via SAML



Use case details – Web SSO via SAML

Author:	John Tolbert
Brief Description:	Human user requesting access to an html document protected by a web application that accepts SAML assertions. Policy information stored in LDAP, authored within LDAP/SAML/other utilities.
Goal:	Human user gains access to authorized document or application.
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	User clicks link to protected resource
Steps or flow:	User clicks link to protected html resource; SAML assertion with appropriate attributes created and passed to application; application on host system asks PDP if the user can get access; PDP relies on pre-authored LDAP policy data; PDP returns result to PEP, host system delivers document to user.
Post-conditions:	Transaction logged.
Non-functional requirements:	
Business rules:	Optional rules to consider include regulations (export, HIPAA, SOx), privacy, intellectual property controls, national security, need-to-know, etc.
Issues:	PEP and PDP deployments in this case are limited to platforms served by the SAML-enabled application.

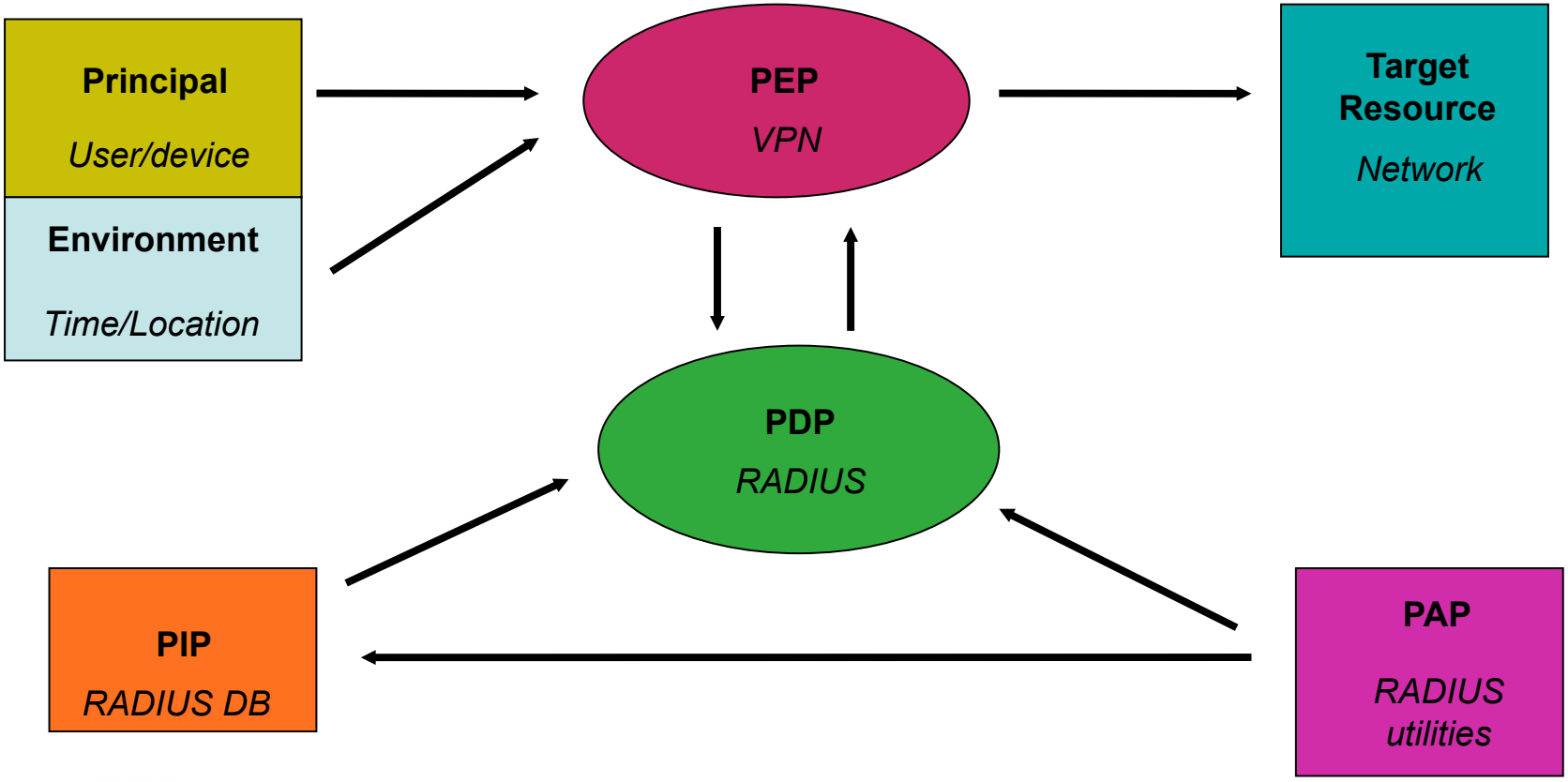
AuthZ Use Case 3 – File access mediated by operating system (OS)



Use case details – File access mediated by operating system (OS)

Author:	John Tolbert
Brief Description:	Human user requesting access to a file controlled by an operating system (OS). Policy information stored within OS structures, authored by OS utilities.
Goal:	Human user gains access to authorized document or application.
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	File created with permissions, access determined in advance by entitlement creation using OS utilities.
Steps or flow:	User attempts to access a file protected by an OS. OS makes decision based upon entitlements created by OS utilities. File delivered to user.
Post-conditions:	Transaction logged.
Non-functional requirements:	
Business rules:	Optional rules to consider include regulations (export, HIPAA, SOx), privacy, intellectual property controls, national security, need-to-know, etc.
Issues:	PEP and PDP deployments in this case are dependent on the OS and its mechanisms.

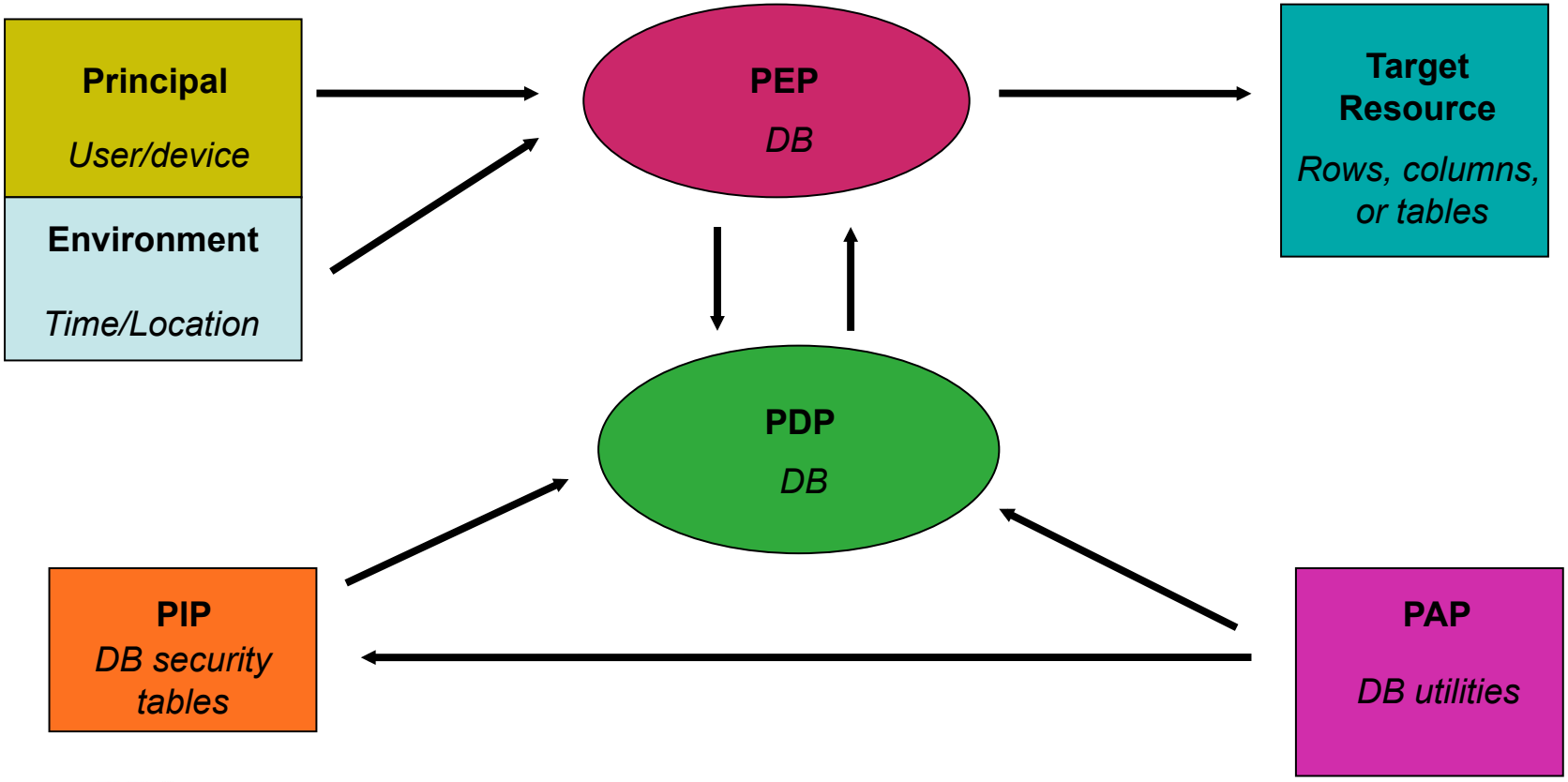
AuthZ Use Case 4 – remote network access to virtual private network (VPN)



Use case details – remote network access to virtual private network (VPN)

Author:	John Tolbert
Brief Description:	Human user and/or requesting access to a network controlled by a VPN device. Policy information stored within RADIUS (or TACACS or LDAP), authored by RADIUS utilities.
Goal:	Human user gains access to authorized network.
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	Entitlements created in advance by RADIUS utilities. VPN client software installed.
Steps or flow:	User attempts to access a remote network. VPN device makes decision based upon entitlements created. Network access granted to user.
Post-conditions:	Transaction logged.
Non-functional requirements:	
Business rules:	Optional rules to consider include regulations (export, HIPAA, SOx), privacy, intellectual property controls, national security, need-to-know, citizenship, etc.
Issues:	PEP and PDP deployments in this case are dependent on the OS and its mechanisms.

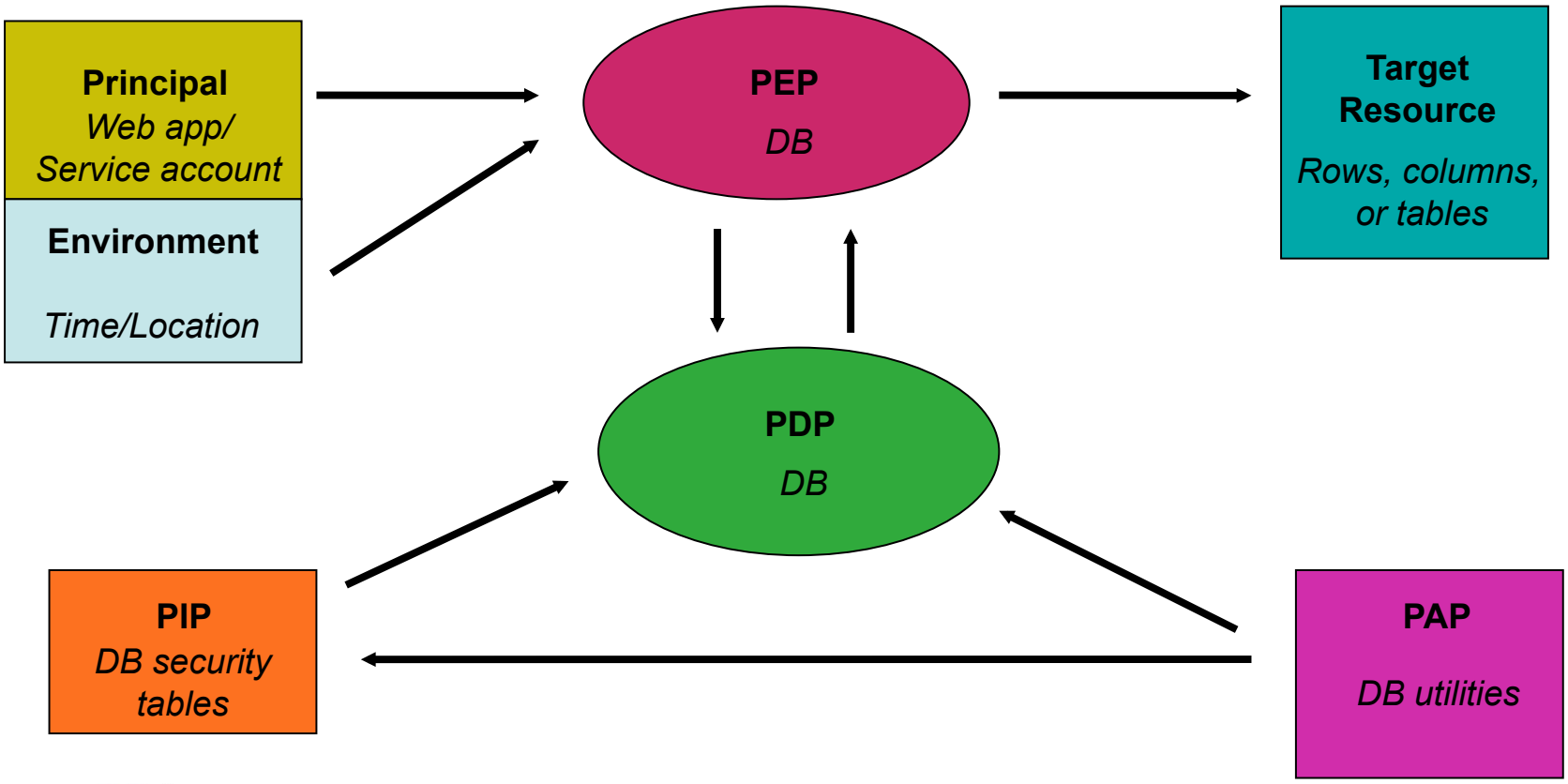
AuthZ Use Case 5 – Database access using local DB accounts



Use case details – Database access using local DB accounts

Author:	John Tolbert
Brief Description:	Human user requesting access to data stored in a database. Policy information stored in internal database security structures (user, group, permissions tables), created by DB utilities.
Goal:	Human user gains access to authorized document or application.
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	User executes SQL query against database.
Steps or flow:	User executes SQL query against database. Database security functions match user context information against pre-configured values in the user, group, and permissions table structures within the database itself. If conditions are met, results will be returned.
Post-conditions:	Transaction logged.
Non-functional requirements:	
Business rules:	Optional rules to consider include regulations (export, HIPAA, SOx), privacy, intellectual property controls, national security, need-to-know, etc.
Issues:	PEP and PDP deployments in this case are limited to platforms which can operate within the database program.

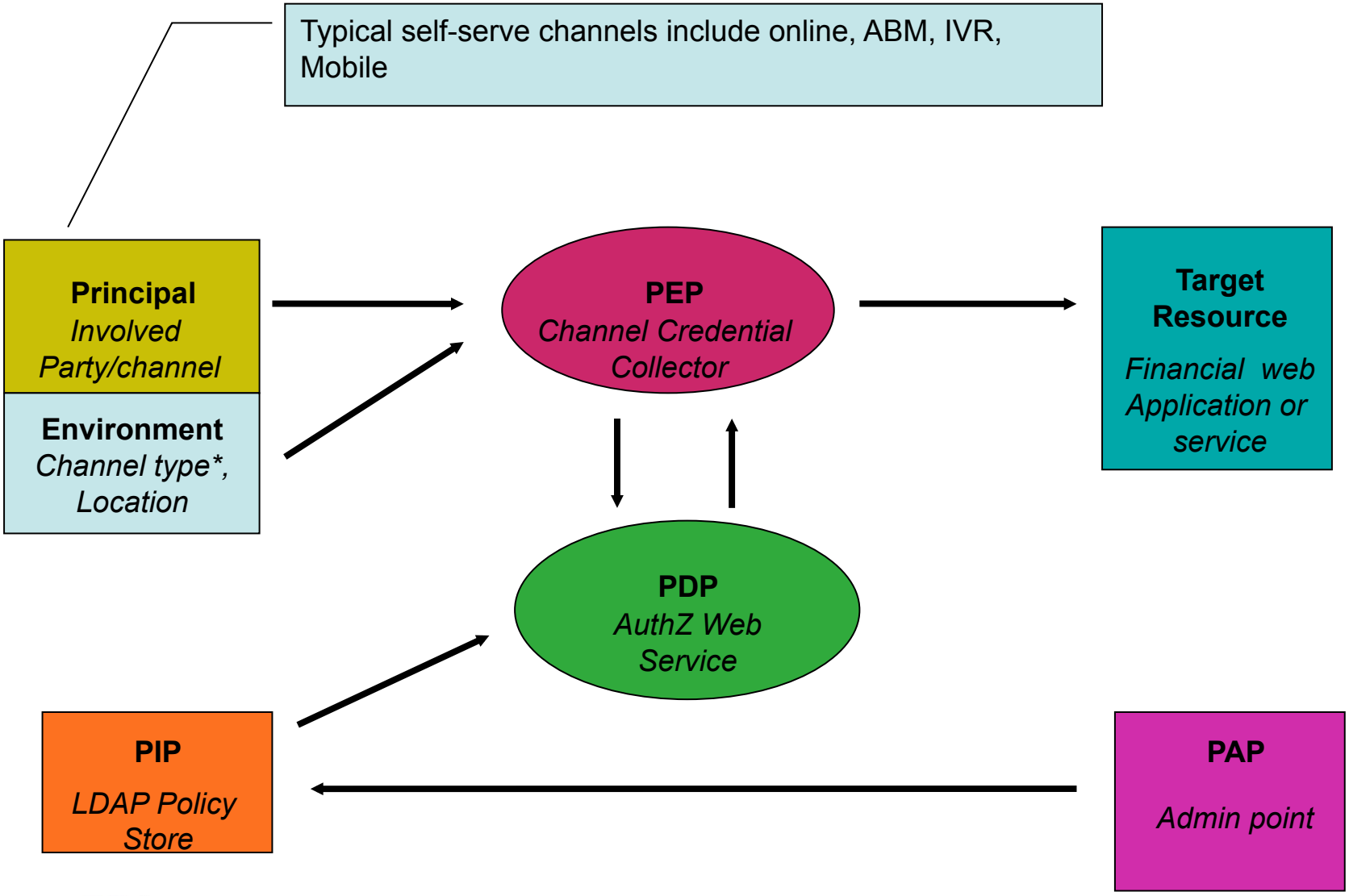
AuthZ Use Case 6 – Database access via web application



Use case details – Database access using Database access via web application

Author:	John Tolbert
Brief Description:	Human user requesting access to data stored in a database via a web application. Policy information stored in internal database security structures (user, group, permissions tables), created by DB utilities.
Goal:	Human user gains access to authorized document or application.
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	User clicks link in web application that launches a SQL query against a back-end database.
Steps or flow:	User clicks link in web application that launches a SQL query against a backend database. Web application executes SQL query on behalf of the user, either using impersonation or a service account. Database security functions match user or service account context information against pre-configured values in the user, group, and permissions table structures within the database itself. If conditions are met, results will be returned.
Post-conditions:	Transaction logged.
Non-functional requirements:	
Business rules:	Optional rules to consider include regulations (export, HIPAA, SOx), privacy, intellectual property controls, national security, need-to-know, etc.
Issues:	PEP and PDP deployments in this case are limited to platforms which can operate within the database program. WAM may also front-end the web application.

AuthZ Use Case 7: Multi-channel access to financial service



Use case details: Multi-channel access to financial services

Author:	Gavin Illingworth
Brief Description:	Involved Party (IP) is a subject who may play a role of (bank) customer, guarantor, trustee or similar. IP uses bank-issued credentials to first authenticate to a channel. IP is then authorized to access one or more services. Which services are permitted depends on the following factors:
Goal:	Managed access to financial applications
Actors:	User, PEP, PDP, PIP, PAP, resource.
Initial conditions:	Subject has authenticated to a channel. Subject has been assigned several credentials of varying strength.
Steps or flow:	1. Subject authenticates to channel 2. Authentication Service gets channel properties, credential, credential type and assurance level of identity 3. The assurance level assigned to a subject at registration time (depends on bona fides, such as driver's license, submitted by the subject at a branch). This is a static value 4. A session assurance level is calculated as determined by the strength of the supplied credential and channel properties, such as channel type and location 5. Uses authorization rules in the Policy Store to calculate decisions 6. The session assurance value is used (in prior step) to assess what entitlements are 'operational' during the session. 7. Returns authorization decision back to the invoking applications. 8. The "conditional" return value may result in a request to the customer/user to provide additional credentials to increase the session assurance level (stronger credential). 9. Subject may be granted resource access

Use case details: Multi-channel access to financial service (2)

Business rules:	
Issues:	The list of services during a session is not fixed, but is dynamically calculated as shown. The implication for the UI is that, although there is a list of (all) available services determined by entitlements (at enrolment time), the authorization decision during a session may render some of them non-permissible. Do you present both and remind the subject that additional AuthN is required for any services greyed out in the session? Or do you present only the ones permissible for that AuthZ decision?