Implementing Privacy

Using the OASIS XACML Standard to implement privacy using attribute-based access control

Externalizing Authorization

Introduction to XACML

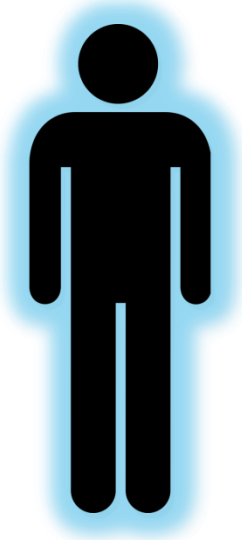
XACML & Privacy

Customer use cases

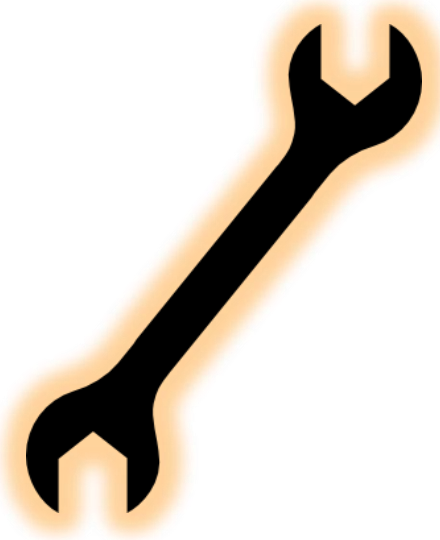
Externalizing Authorization

Next Generation Authorization
Attribute Based Access Control

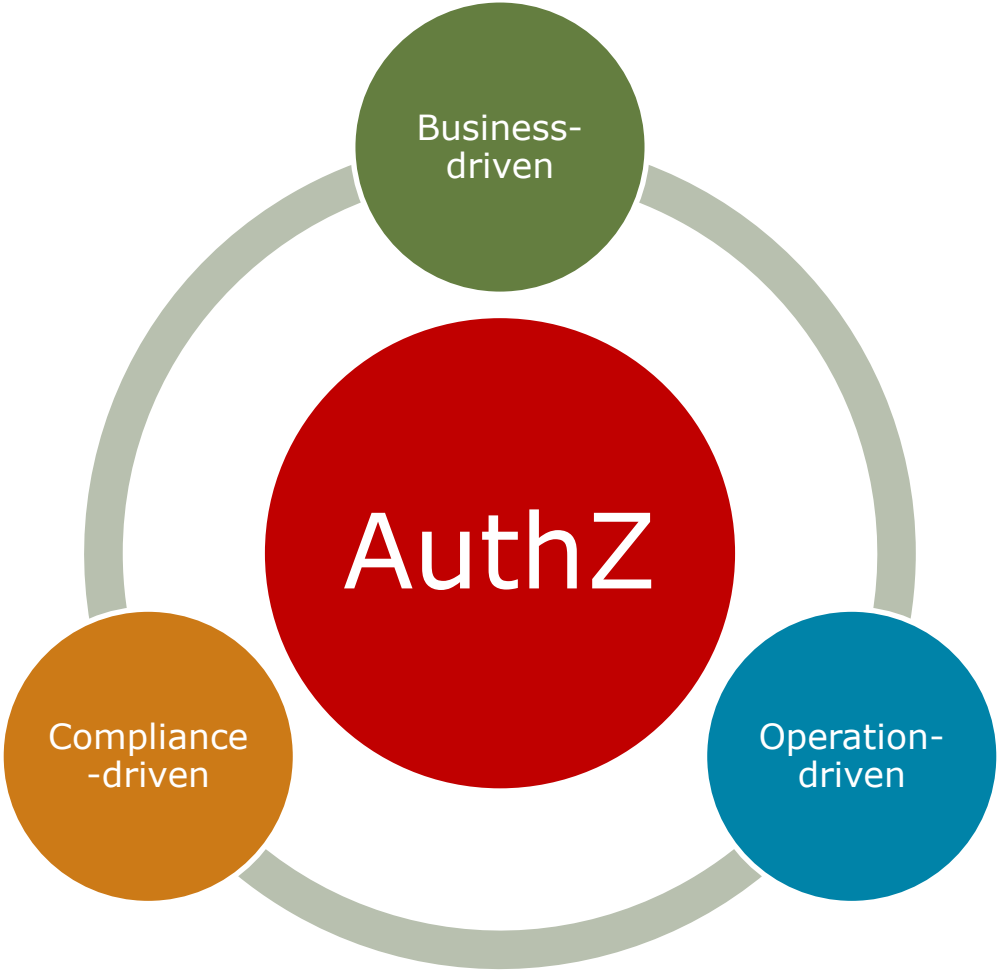
Authentication & Authorization



Authentication:
Determine who the user is



Authorization:
Determine what the user can do



Examples

- Business-driven
  - Finance: A junior teller can approve transactions up to 1,000 USD.
  - Healthcare: A senior nurse can edit the notes of a medical record.
- Operations-driven
  - Finance: No one can approve transactions between 5pm and 9am.
  - Healthcare: No one can print a medical record from home.
- Compliance-driven
  - Finance: a trader cannot approve a trade order he created (segregation of duty)
  - Healthcare: mask the social security number on the X-ray print-out

This is where privacy fits in.

Privacy-enabling authorization: requirements

- A bank customer wants their account information to be available to bank staff.
  - So long as their access is motivated by services they provide the customer
- The customer doesn't want bank staff to access the data for other reasons
  - E.g. gossip
- For privacy, CONTEXT IS KEY.
  - A staff member viewing a record may be aligned with privacy requirements on Monday…
  - But violating them on Tuesday.
- How do existing authorization frameworks cater for context?
  - They don't
  - We need to look for a new framework or model?

Challenges with existing authorization solutions

- User-centric only
- Software-specific
- Static
- Lack of visibility → difficult to audit the system
- Cannot cater for context
- Cannot evolve to meet new business needs
- Expensive
- Developers don’t like it

The need for next-generation authorization

External from applications

- Decouple business logic implementation from authorization logic

Standards-based

- OASIS XACML: eXtensible Access Control Markup Language

Fine-grained

- It's not just about who the user is, it's about who, what, when, where, why, and how

Context-aware

- Context matters: time of day, device, purpose of use…

Attribute-based Access Control (ABAC)

Implement privacy with Attribute-based access control

Doctors should be able to view the records of patients assigned to their unit and edit the records of those patients with whom they have a care relationship

Privacy by design: ONLY authorized persons can access/update the record

ABAC takes multiple factors into account

- Not just users and roles…
  … but also **attributes** reflecting the business process and context

- **Policies** define precise access rules….
  … which are **dynamically enforced in real-time**

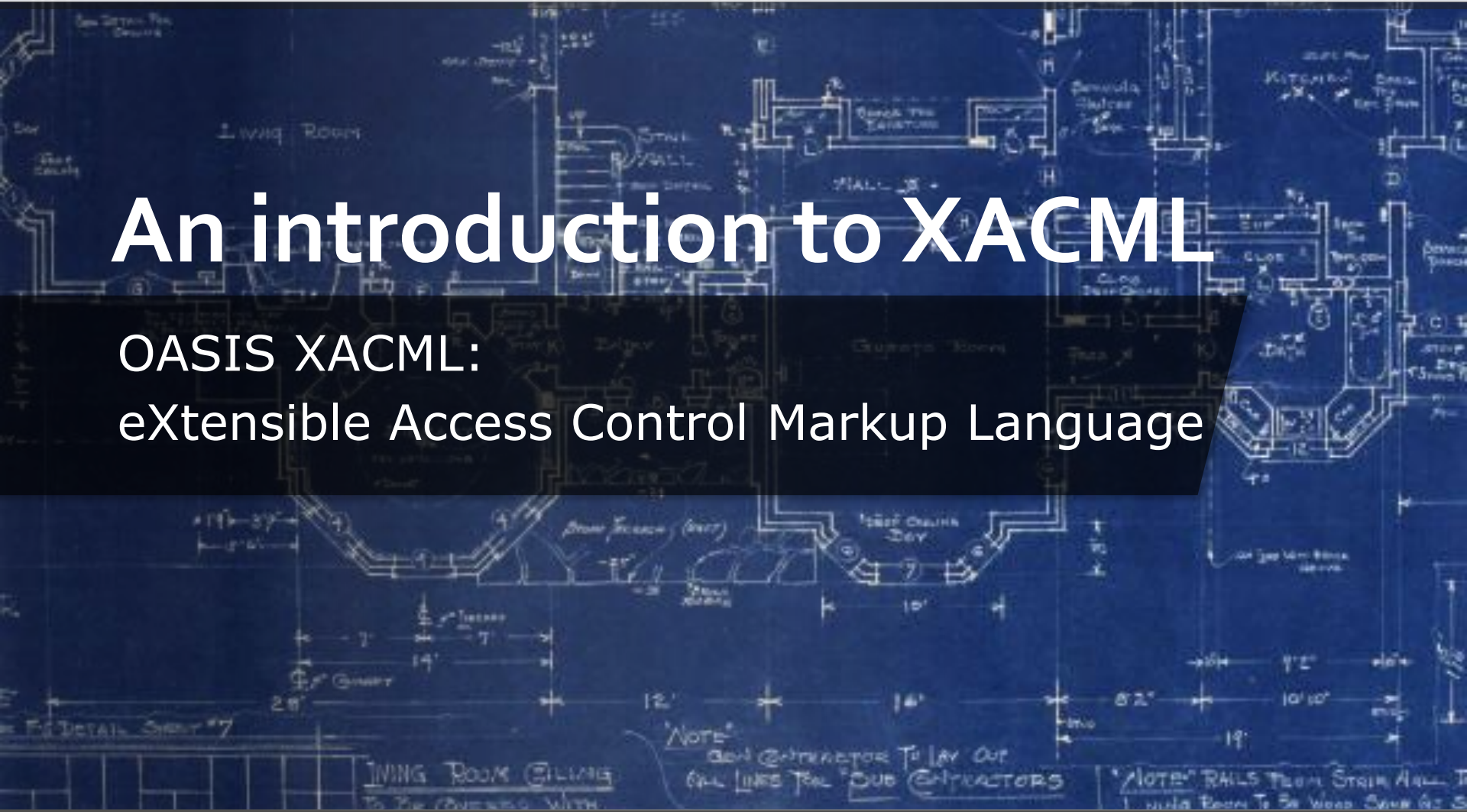
Attribute-Based Access Control

Example: Doctors can open & edit a patient's health record in the hospital emergency room between 5PM and 8 AM.

Read more here:
csrc.nist.gov/projects/abac/

Externalized Authorization Management Benefits

- User-, Resource-, Relationship-centric: *-based access control
- Standards-based, generic: implemented on top of OASIS XACML
- Dynamic: adapt to change and context
- Centrally managed authorization: all authorization policies are in one place
- Context is one of the parameters: take time, location and device into account
- Adapts to new requirements: authorization policies can grow independently
- Reusable, cost-effective: write once, enforce everywhere
- Easy on developers: developers no longer need to worry about authorization.



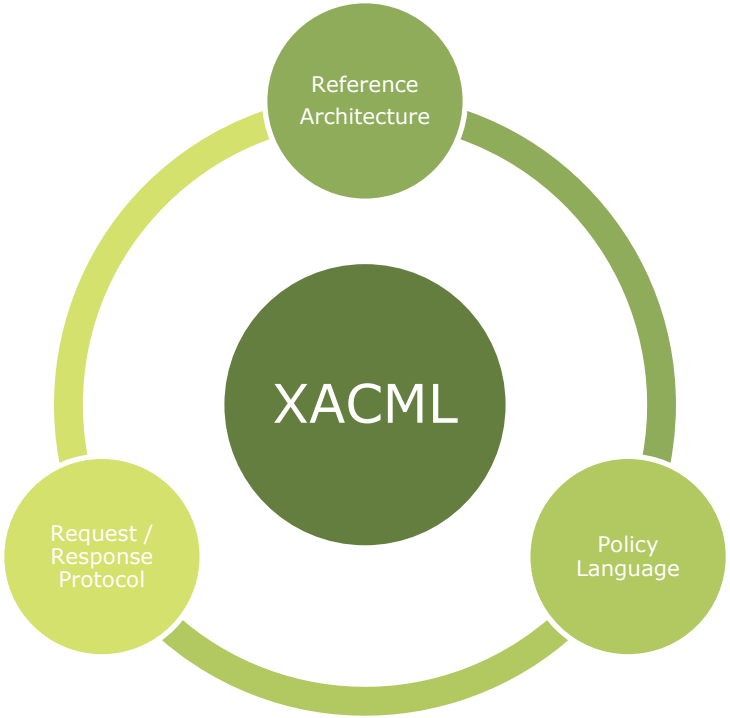
An introduction to XACML

OASIS XACML:
eXtensible Access Control Markup Language

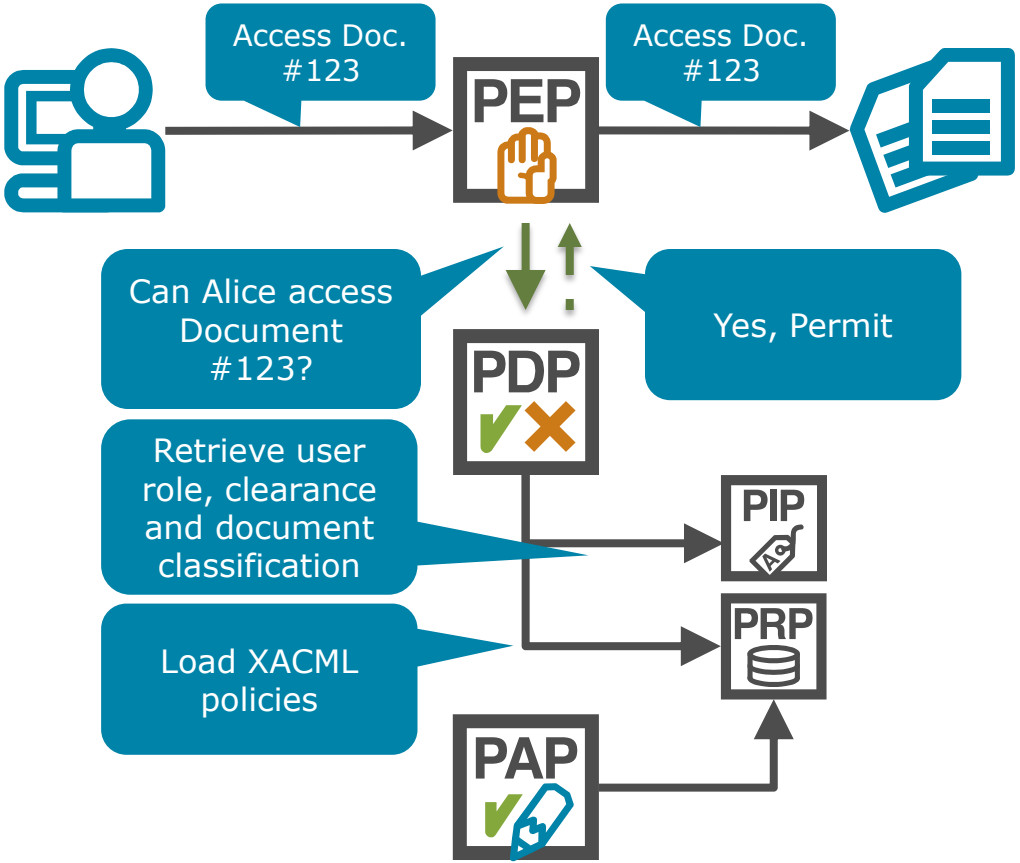
What is XACML?

- Pronunciation
- eXtensible Access Control Markup Language
- OASIS standard
  - V 3.0 approved in January 2013
  - V 1.0 approved in 2003 (11 years ago!)
- XACML is expressed as
  - A specification document and
  - An XML schema
- http://www.oasis-open.org/committees/xacml/

What does XACML contain?



The XACML Architecture & Flow



Enforce
Policy Enforcement Point

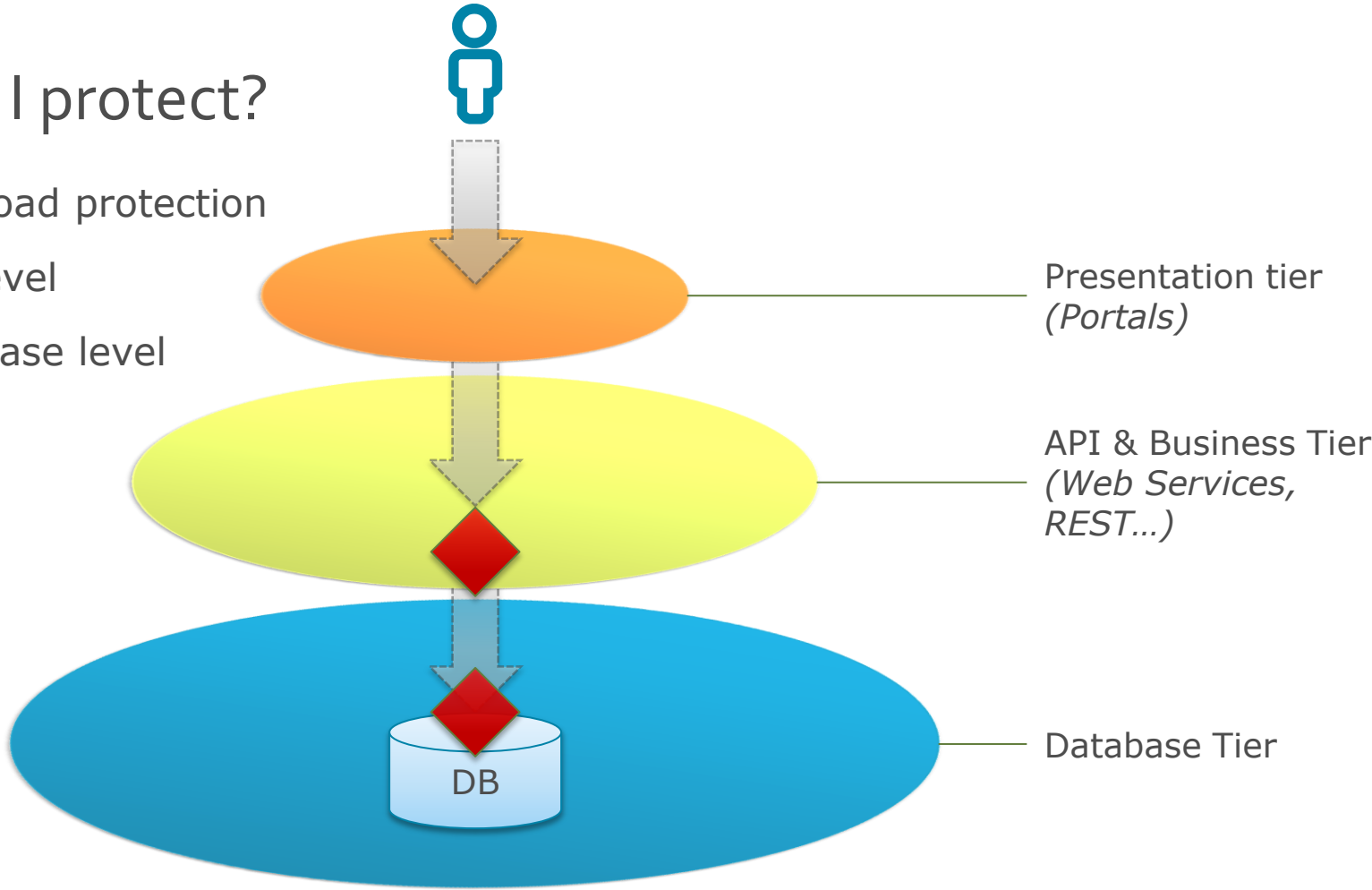
Decide
Policy Decision Point

Support
Policy Information Point
Policy Retrieval Point

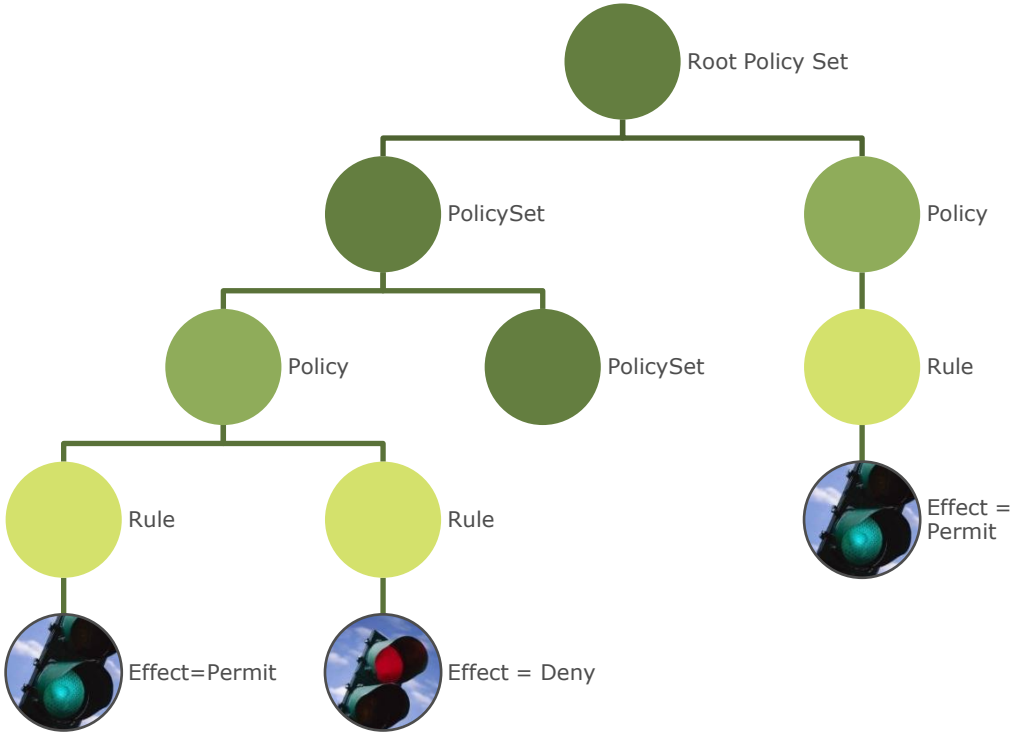
Manage
Policy Administration Point

Where do I protect?

- Choose a broad protection
- At the API level
- At the database level



Sample XACML Policy



XACML & Privacy

Using XACML to implement various privacy regulations

XACML profiles on privacy

- Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML for Healthcare (link)
  - This profile provides a cross-enterprise security and privacy profile that describes how to use XACML to provide privacy policies and consent directives in an interoperable manner.
- Cross-Enterprise Security and Privacy Authorization (XSPA) profile of XACML v2.0 for Healthcare, Implementation Examples (link)
  - This profile takes HL7 examples and converts to XACML
- Privacy policy profile of XACML v2.0
  - Based on the Organization of Economic Cooperation and Development (1980) privacy guidelines
- Other regulations on data protection (not specific to privacy)
  - XACML Intellectual Property Control (IPC) Profile
  - XACML 3.0 Export Compliance-US (EC-US) Profile

HL7 Security and Privacy Ontology Use Cases

link

```
/*
 * Access Control Based on Category of Action
* Access to progress notes
 */
policy progressNotes{
target clause objectType=="progress note"
apply firstApplicable
        /*
         * A primary physician can create a patient's progress note
         */
        rule createNote{
        target clause role=="physician" and action=="create"
        condition primaryPhysician==requestorId
        permit
        }
}
```

(the above is ALFA – a XACML pseudo-code. Download ALFA here.)

XACML & the 7 Foundational Principles (1/2)

Proactive not Reactive; _Preventative_ not Remedial

- XACML defines an architecture enacted at runtime

Privacy as the _Default Setting_

- XACML policies enable exact privilege settings

Privacy _Embedded_ into Design

- IT projects can focus on authorization requirements on the one hand and business requirements on the other
- Clear separation of concerns

XACML & the 7 Foundational Principles (2/2)

Full Functionality — *Positive-Sum*, not Zero-Sum

- XACML is a business enabler
- It allows for data to be securely shared
- XACML helps deliver new services

End-to-End Security — *Full Lifecycle Protection*

- XACML policies evolve with the data they protect
- XACML policies can adapt to regulatory change

Visibility* and *Transparency* — Keep it *Open

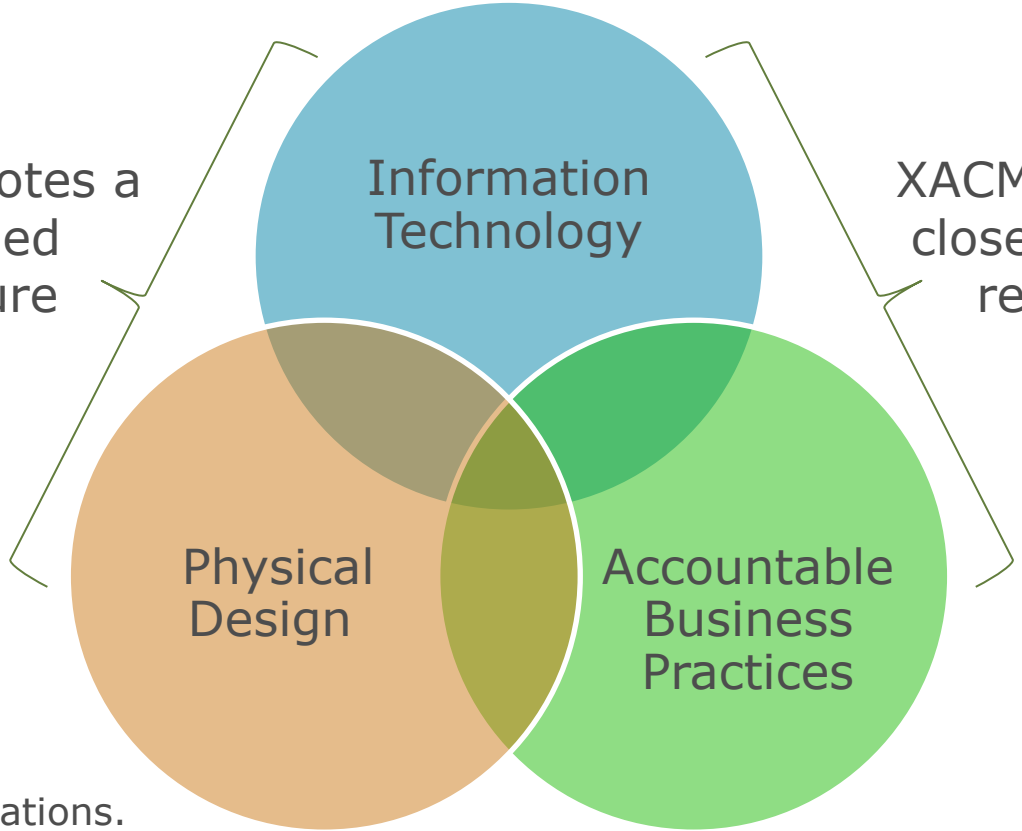
- XACML policies are centrally managed and can be easily audited
- XACML policies mirror business requirements closely

Respect* for User Privacy — Keep it *User-Centric

- XACML policies focus on the entire picture: from who is accessing the data to the relationships to the purpose of use…

Privacy by Design: Trilogy of Applications & XACML

XACML promotes a well-defined architecture



XACML policies map closely to business requirements

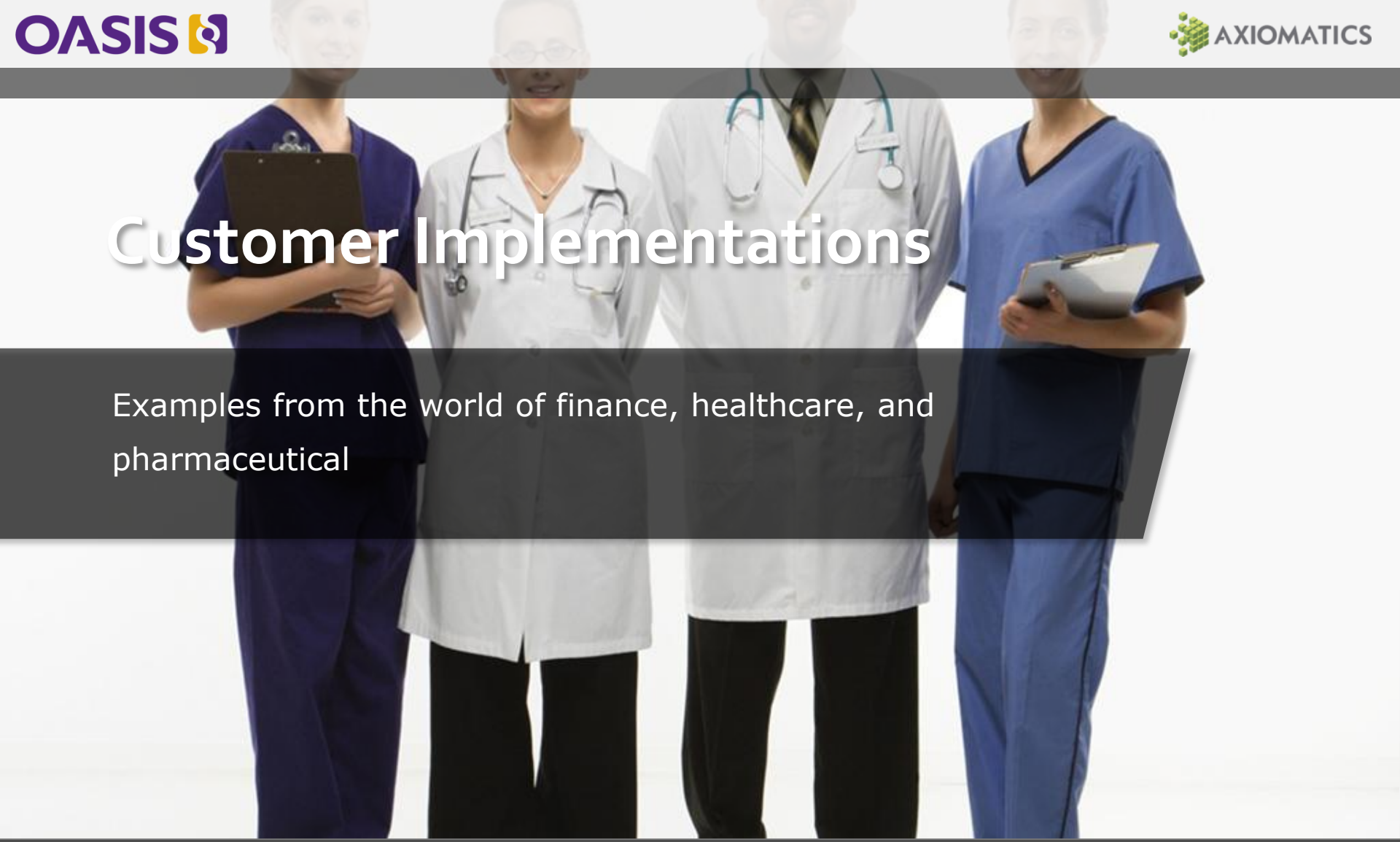
Watch Ann Cavoukian on the Trilogy of Applications.

XACML enables the positive-sum

- Example: medical records
  - Medical records used to be stored in a physical location at the doctor's office.
  - Security was there by default: it is hard to access information stored in a file cabinet
- Today: new consumer & medical patterns emerge
  - Let patients browse their medical data online
  - Share data with other medical actors (hospitals, specialists, pharmacies…) and non-medical actors (insurance companies…)
  - The promise: deliver better care
- XACML, as an IT security artefact, can help go from high-level privacy designs to technical implementations

Key take-aways

- Privacy is more about controlled information sharing than the prevention thereof ➔ XACML enables secure information sharing
- The privacy headache will explode once the new EU regulation becomes reality ➔ industries will need a means to quickly and efficiently implement privacy. XACML is the way to go on a technical level
- Privacy is not just about compliance, it's also about
  - Brand
  - Reputation, and
  - Trust.
- A key challenge is that privacy is a human concept. XACML bridges the gap between human & business requirements and technical implementations



Customer Implementations

Examples from the world of finance, healthcare, and pharmaceutical

Norwegian bank (1/2)

- Lov om behandling av personopplysninger (personopplysningsloven | link)
- Datatilsynet (Norwegian Data Protection Authority) requires:
  - that bank clients should be able to demand exact records of which staff member accessed their account details or other privacy sensitive data and when this happened
  - that the bank must ensure that only staff members with a purpose of use motivated by tasks performed in the course of their professional duties access sensitive data. The bank must be able to investigate any suspicions that this rule is being violated by staff members.
  - that the bank duly considers the risk assessment mandates of the legislation must be recognized (for instance with regard to VIP accounts or accounts of citizens with a protected identity due to witness protection etc.)
- The project used XACML to implement fine-grained access control in conformance with privacy regulations

Norwegian bank (2/2) Details

- A whitelist is defined: customers have the right to define who can access their data
- A blacklist is defined: customer have the right to define who cannot access their data
  - E.g. relatives…
- Common rules are implemented
  - Only employees in a given branch can view customer data from that branch
- Exception handling and flags are implemented
- All access to data is logged for future accountability

Swedish National Healthcare

- Project driven by the Swedish Medical Care Advice Service
  - Goal: comprehensive IT-solution for electronic patient record management
  - Uniform technical choices for future security services
- Excerpt from the general goals for BIF services
  - Provide access to authorized personnel
  - Protect sensitive patient data against unauthorized access
- Functional requirements
  - Strong emphasis on standard based approaches
  - E.g. XACML shall be used for access control
- World's largest deployment of XACML yet

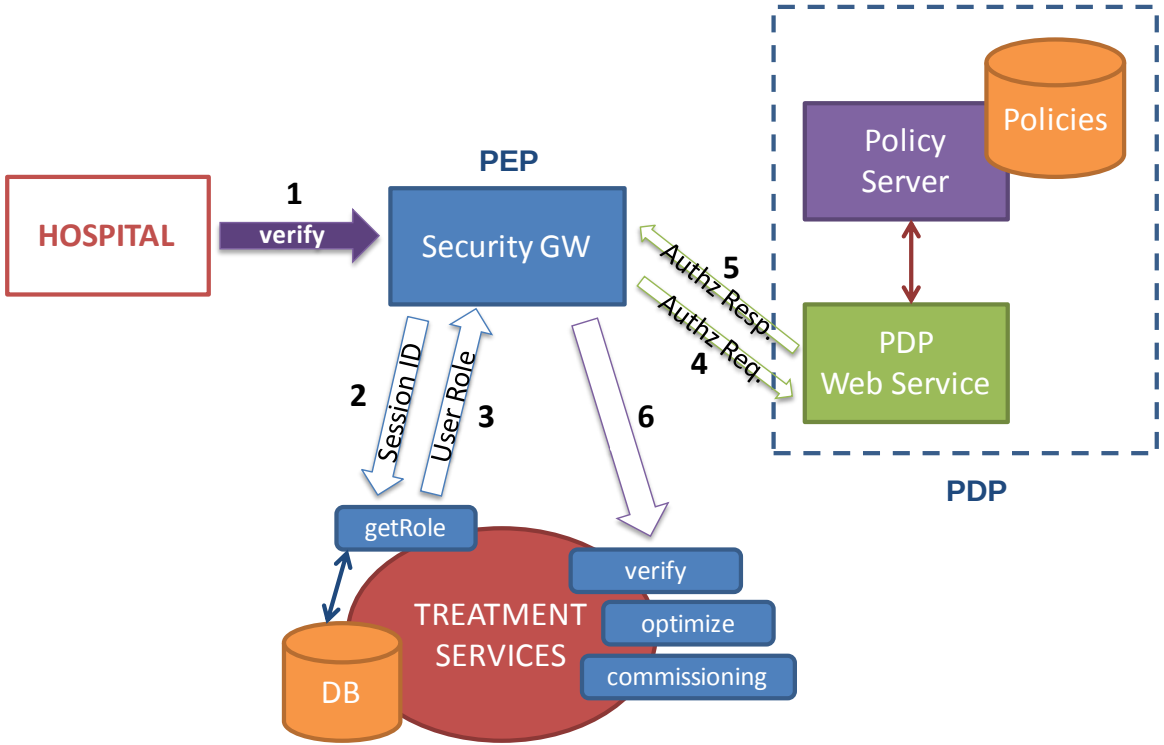
Swedish National Healthcare: access control rules

- At the medical center level
  - Only doctors that belong to the given medical center can see records of patients from that medical center
- At the district level
  - Only doctors that belong to the given district can see records of patients from that district
  - Patients can define their own policies: patient-defined disclosure policies (pddp)
- At the top level – the organization
  - Patients need to provide an additional consent form for their data to be disclosed
  - An emergency plan provides for exceptional policies to override patient-defined rules

Northern Spain Hospitals Cancer Treatment (1/2)

- BEinGRID: EU-funded development of Business Models for the Grid Industry.
- Healthcare business use case
  - Provide new compute intensive radiotherapy tools to hospitals remotely
  - Challenge: A new treatment needs several hours or days.
  - Goal: drive down the time it takes to design radiotherapy treatments
- Privacy?
  - Radiotherapy records contain Personal Health Information (PHI) that must be stripped before the records can be sent to the super computers
- Read more
  - Link

Northern Spain Hospitals Cancer Treatment (2/2)



US Pharmaceutical

- Goal: share medical information (clinical trials, molecule…) with partners, contractors, universities, and authorities
- Privacy?
  - Clinical trials contain highly sensitive PHI.
  - For the customer the alternative is not sharing the data at all to avoid breaches & fines.

More examples here at EIC 2014

- Drivers and Lessons learned from a Recent ABAC Implementation at Generali
  - Manuel Schneider, Generali
  - 14.05.2014 14:30-15:30
- ABAC - Visions and Reality
  - Finn Frisch, Axiomatics
  - 14.05.2014 14:30-15:30
- Dynamic Authorization Management: The Market and its Future
  - Graham Williamson
  - 14.05.2014 12:00-13:00
- RBAC, ABAC, or Both?
  - Panel
  - 14.05.2014 12:00-13:00

Thank you.