[l02] know what we are protecting

[l02_t01] modeling

wim mees

introduction

learning objectives

- understand the mapping of
  "business" activities to IT infrastructure
  (and back)
- able to model at "business" level
- able to model at "information and application" level
- able to model at "technology and infrastructure" level

reference documentation

- course book *"Pragmatic cybersecurity"*
  chapter 1 *"Know what you are protecting"*

what security is not

Figure 1: a product-oriented solution raising false expectations

what security is

Figure 2: a continuous multi-disciplinary team effort

business processes

know what you are protecting

- resources are always limited,
  therefore we need to make choices
- choices to a large extent situated at infrastructure level,
  yet must be based on “business” priorities
- therefore we need to establish a mapping between
  “the business” and “the infrastructure”

from business to infrastructure

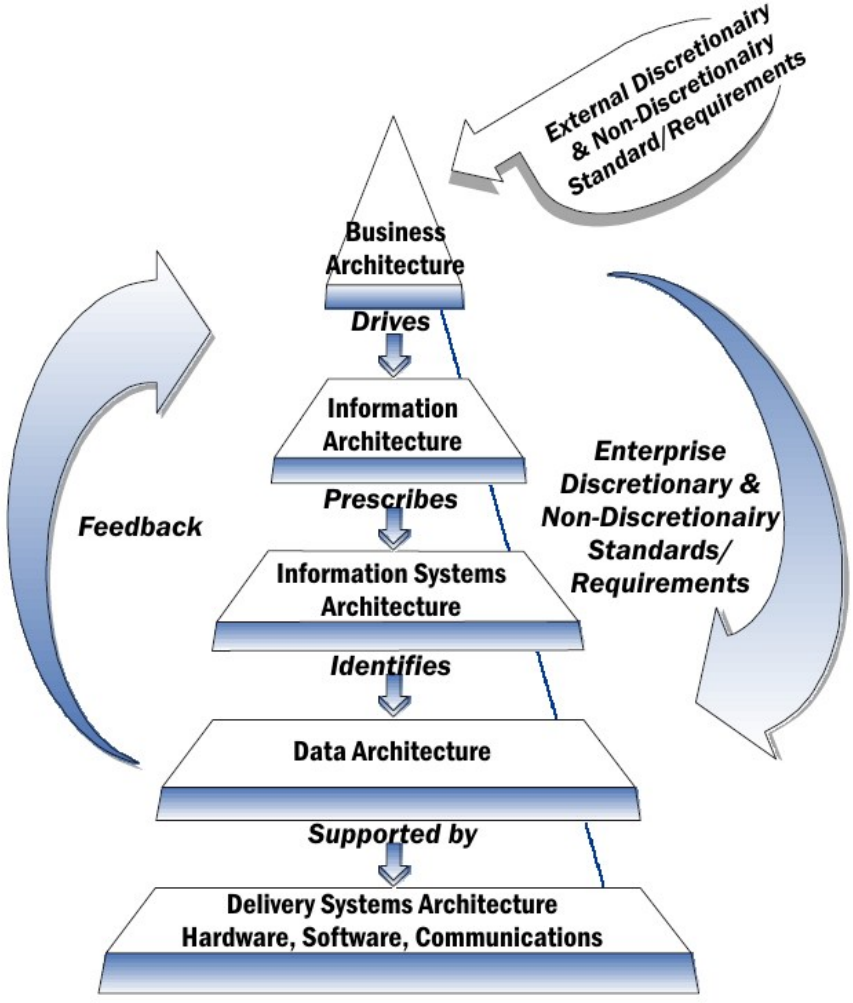


Figure 3: NIST enterprise architecture model

from business to infrastructure

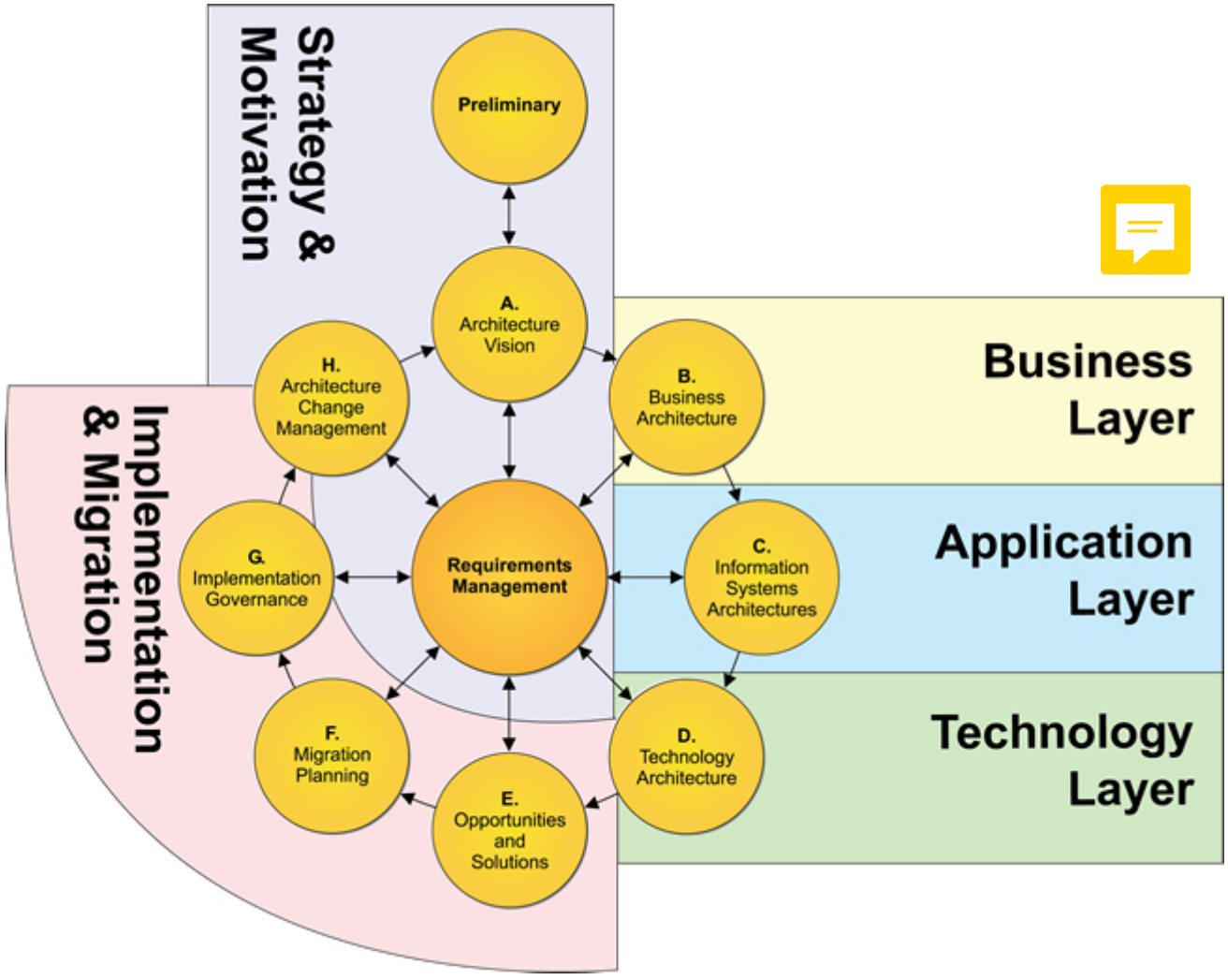


Figure 4: TOGAF enterprise architecture model

from business to infrastructure

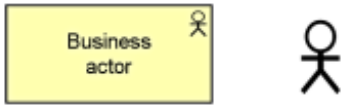
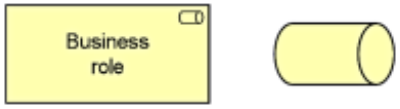
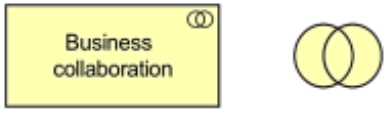
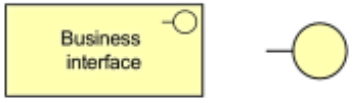
Element	Description	Notation
Business actor	Represents a business entity that is capable of performing behavior.	
Business role	Represents the responsibility for performing specific behavior, to which an actor can be assigned, or the part an actor plays in a particular action or event.	
Business collaboration	Represents an aggregate of two or more business internal active structure elements that work together to perform collective behavior.	
Business interface	Represents a point of access where a business service is made available to the environment.	
Business process	Represents a sequence of business behaviors that achieves a specific result such as a defined set of products or business services.	
Business function	Represents a collection of business behavior based on a chosen set of criteria (typically required business resources and/or competencies), closely aligned to an organization, but not necessarily explicitly governed by the organization.	

Figure 5: Archimate business layer modeling elements

from business to infrastructure

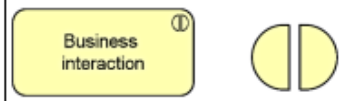
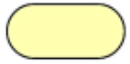
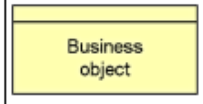
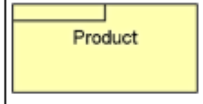
Business interaction	Represents a unit of collective business behavior performed by (a collaboration of) two or more business actors, business roles, or business collaborations.	
Business event	Represents an organizational state change.	 
Business service	Represents explicitly defined behavior that a business role, business actor, or business collaboration exposes to its environment.	 
Business object	Represents a concept used within a particular business domain.	
Contract	Represents a formal or informal specification of an agreement between a provider and a consumer that specifies the rights and obligations associated with a product and establishes functional and non-functional parameters for interaction.	
Representation	Represents a perceptible form of the information carried by a business object.	
Product	Represents a coherent collection of services and/or passive structure elements, accompanied by a contract/set of agreements, which is offered as a whole to (internal or external) customers.	

Figure 6: Archimate business layer modeling elements (cont'd)

from business to infrastructure

- example (from opengroup.org):
  - "Claims Administration" is a business function that is composed of a number of business processes and a business interaction. This business function realizes a "Claims Processing" business service.
  - A business event "Claim Filed" triggers the first business process "Accept Claim", which in turn triggers a business process "Assign Claim".
  - Depending on the type of claim, either the business process "Adjudicate Standard Claim" or the business interaction "Adjudicate High-Risk Claim" is performed. Adjudication of high-risk claims is a business interaction because, according to the company policy, two people should always be involved in this activity to minimize the risk of fraud.
  - After adjudication, the business processes "Notify Customer" and "Pay Claim" are performed in parallel, and when both have finished, business process "Close Claim" is triggered.

from business to infrastructure

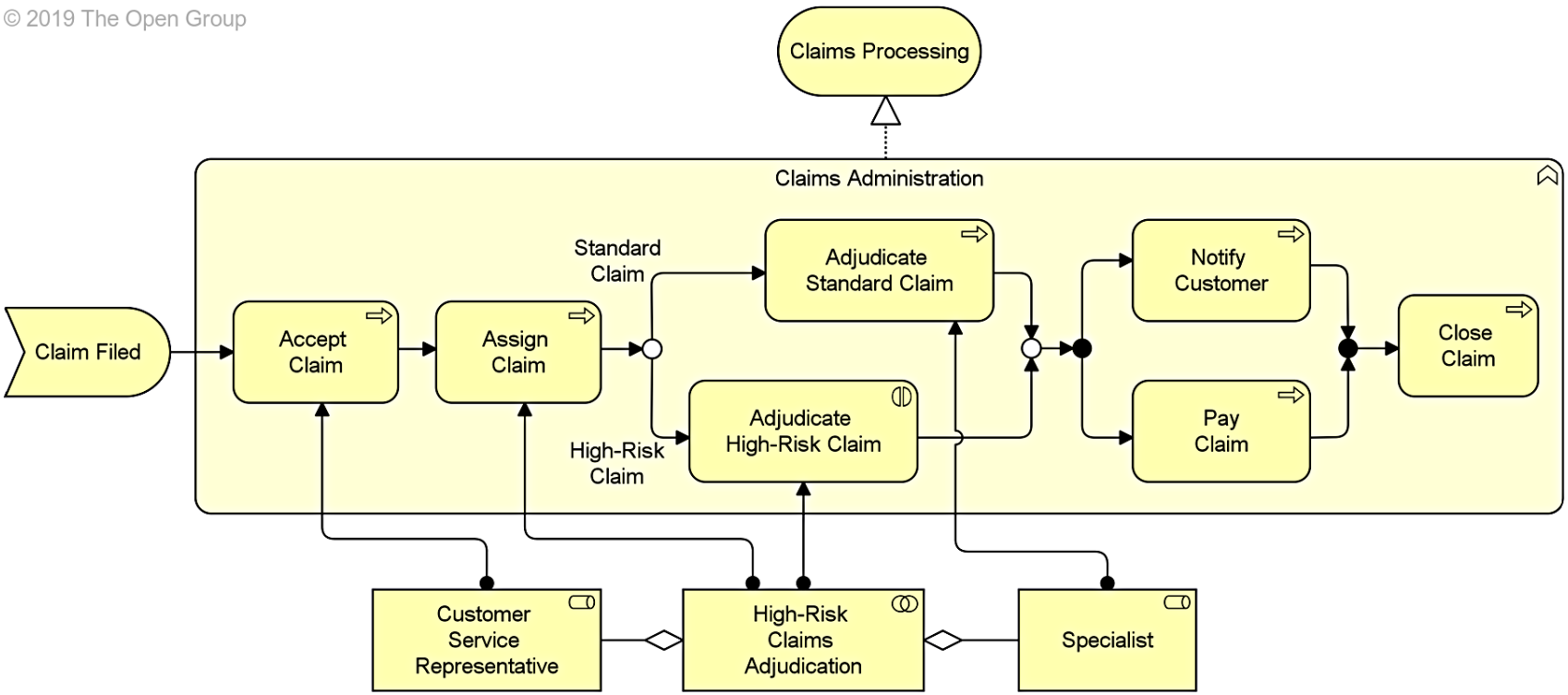


Figure 7: Archimate business layer modeling example (from opengroup.org)

from business to infrastructure

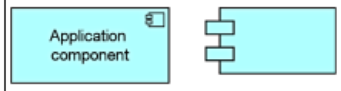
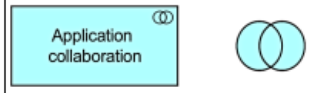
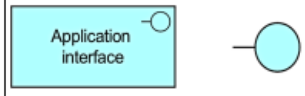
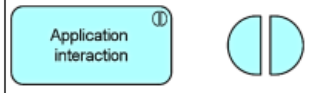
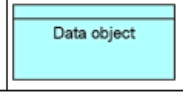
Element	Definition	Notation
Application component	Represents an encapsulation of application functionality aligned to implementation structure, which is modular and replaceable.	
Application collaboration	Represents an aggregate of two or more application internal active structure elements that work together to perform collective application behavior.	
Application interface	Represents a point of access where application services are made available to a user, another application component, or a node.	
Application function	Represents automated behavior that can be performed by an application component.	
Application interaction	Represents a unit of collective application behavior performed by (a collaboration of) two or more application components.	
Application process	Represents a sequence of application behaviors that achieves a specific result.	
Application event	Represents an application state change.	
Application service	Represents an explicitly defined exposed application behavior.	
Data object	Represents data structured for automated processing.	

Figure 8: Archimate application layer modeling elements

from business to infrastructure

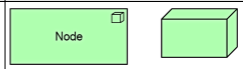
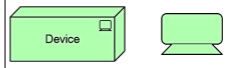
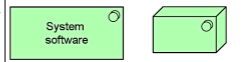
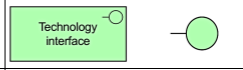
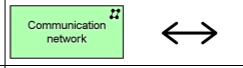
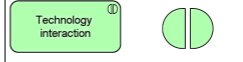
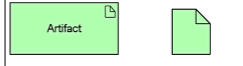
Element	Definition	Notation
Node	Represents a computational or physical resource that hosts, manipulates, or interacts with other computational or physical resources.	
Device	Represents a physical IT resource upon which system software and artifacts may be stored or deployed for execution.	
System software	Represents software that provides or contributes to an environment for storing, executing, and using software or data deployed within it.	
Technology collaboration	Represents an aggregate of two or more technology internal active structure elements that work together to perform collective technology behavior.	
Technology interface	Represents a point of access where technology services offered by a node can be accessed.	
Path	Represents a link between two or more nodes, through which these nodes can exchange data, energy, or material.	
Communication network	Represents a set of structures that connects nodes for transmission, routing, and reception of data.	
Technology function	Represents a collection of technology behavior that can be performed by a node.	
Technology process	Represents a sequence of technology behaviors that achieves a specific result.	
Technology interaction	Represents a unit of collective technology behavior performed by (a collaboration of) two or more nodes.	
Technology event	Represents a technology state change.	
Technology service	Represents an explicitly defined exposed technology behavior.	
Artifact	Represents a piece of data that is used or produced in a software development process, or by deployment and operation of an IT system.	

Figure 9: Archimate technology layer modeling elements

from business to infrastructure

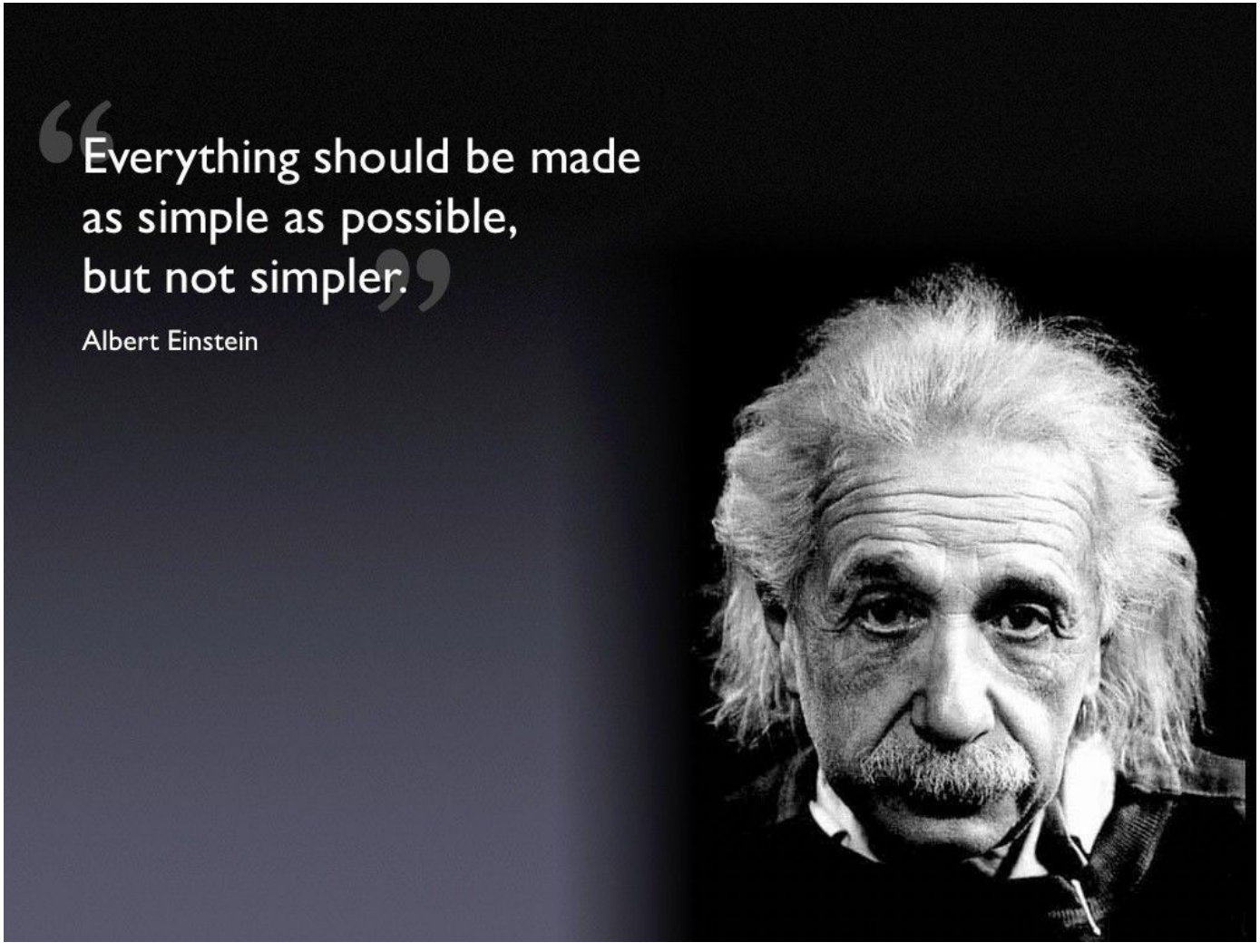


Figure 10: keep it simple, stupid (KISS)

from business to infrastructure

fact check

- you may have already noticed that Einstein “quotes” are very popular and . . . not always correct
- he really said:

  “It can scarcely be denied that the supreme goal of all theory is to make the irreducible basic elements as simple and as few as possible without having to surrender the adequate representation of a single datum of experience.”

(https://championingscience.com/2019/03/15/everything-should-be-made-as-simple-as-possible-but-no-simpler/
)

from business to infrastructure

modeling

- map business down to infrastructure using models, however always remember:

  "All models are wrong but some are useful"

(George Box, statistician, 1978)

- start at highest level of abstraction,
- start with most important "business processes",
- more detailed modeling:
  - only where needed,
  - just-in-time.

business processes

a *"business process"*

- is a collection of "activities" or "tasks",
  typically performed by "actors" playing particular "roles",
  possibly taking certain "decisions",
- consumes certain "resources" and may produce others,
- is sometimes "triggered" by events and
  can generate events to trigger other processes.

a *"business process model"* is a *"process definition"* template,
and is executed as *"process instances"* in the real world.

business process model and notation (BPMN)

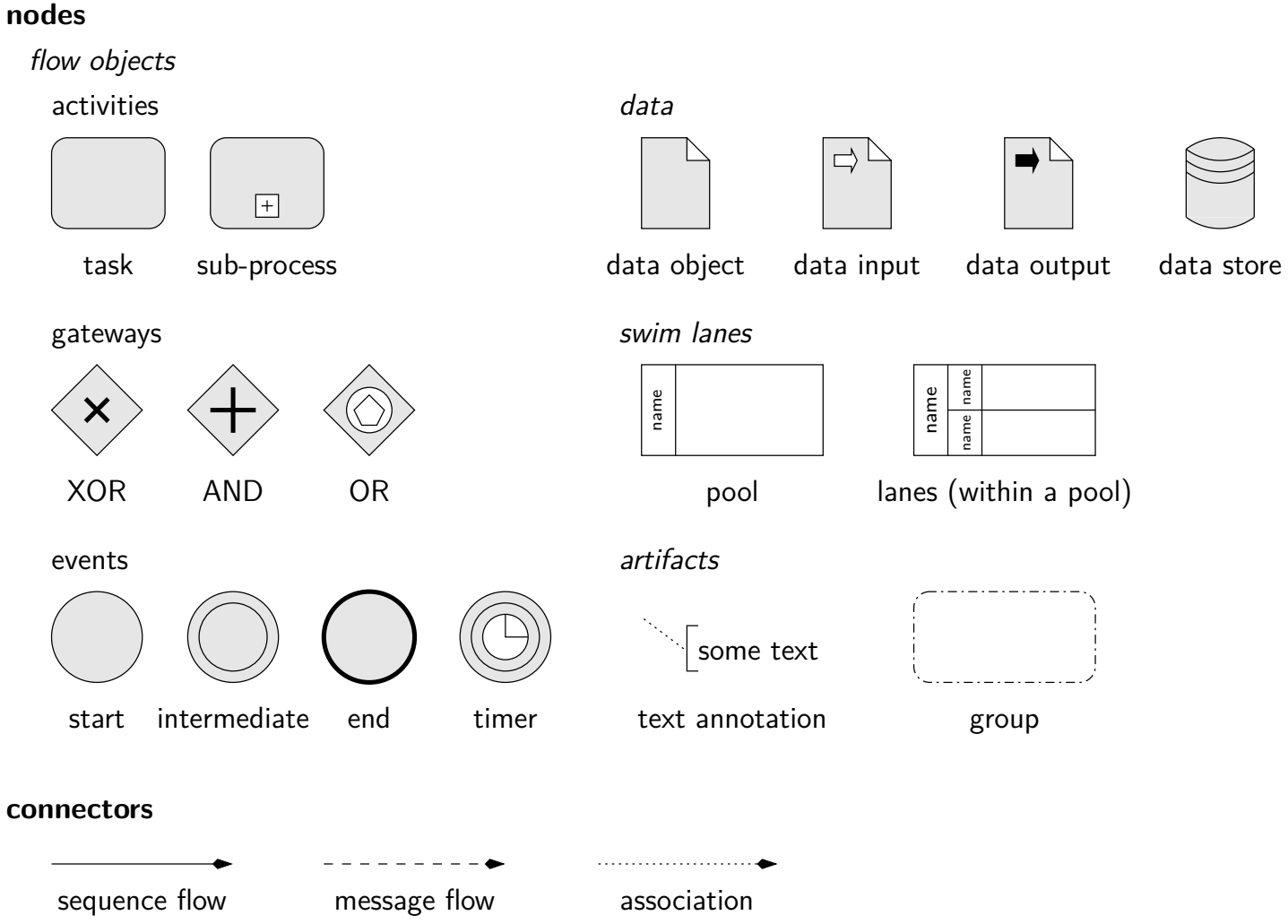


Figure 11: BPMN notation

BPMN

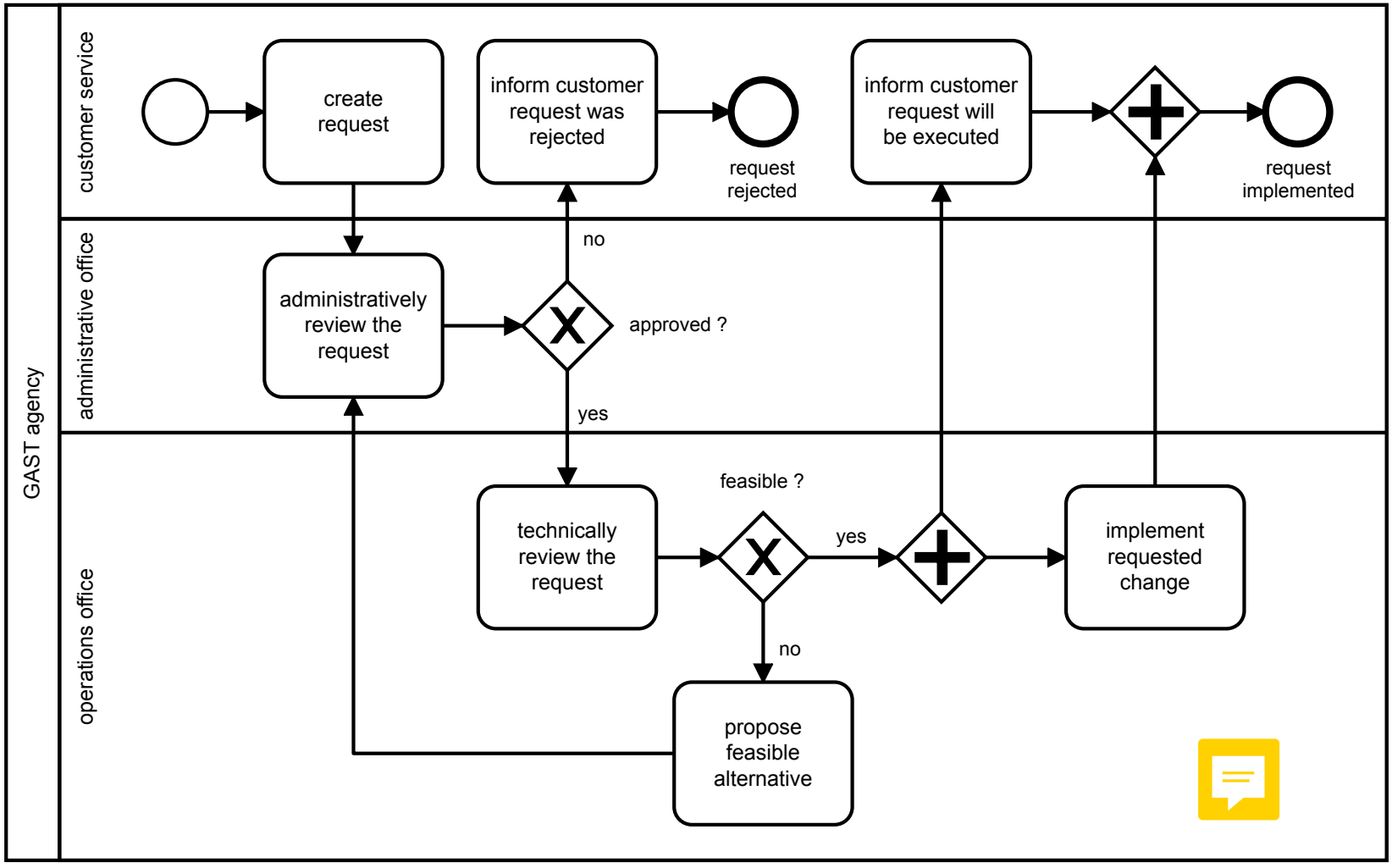


Figure 12: BPMN example

unified modeling language (UML)

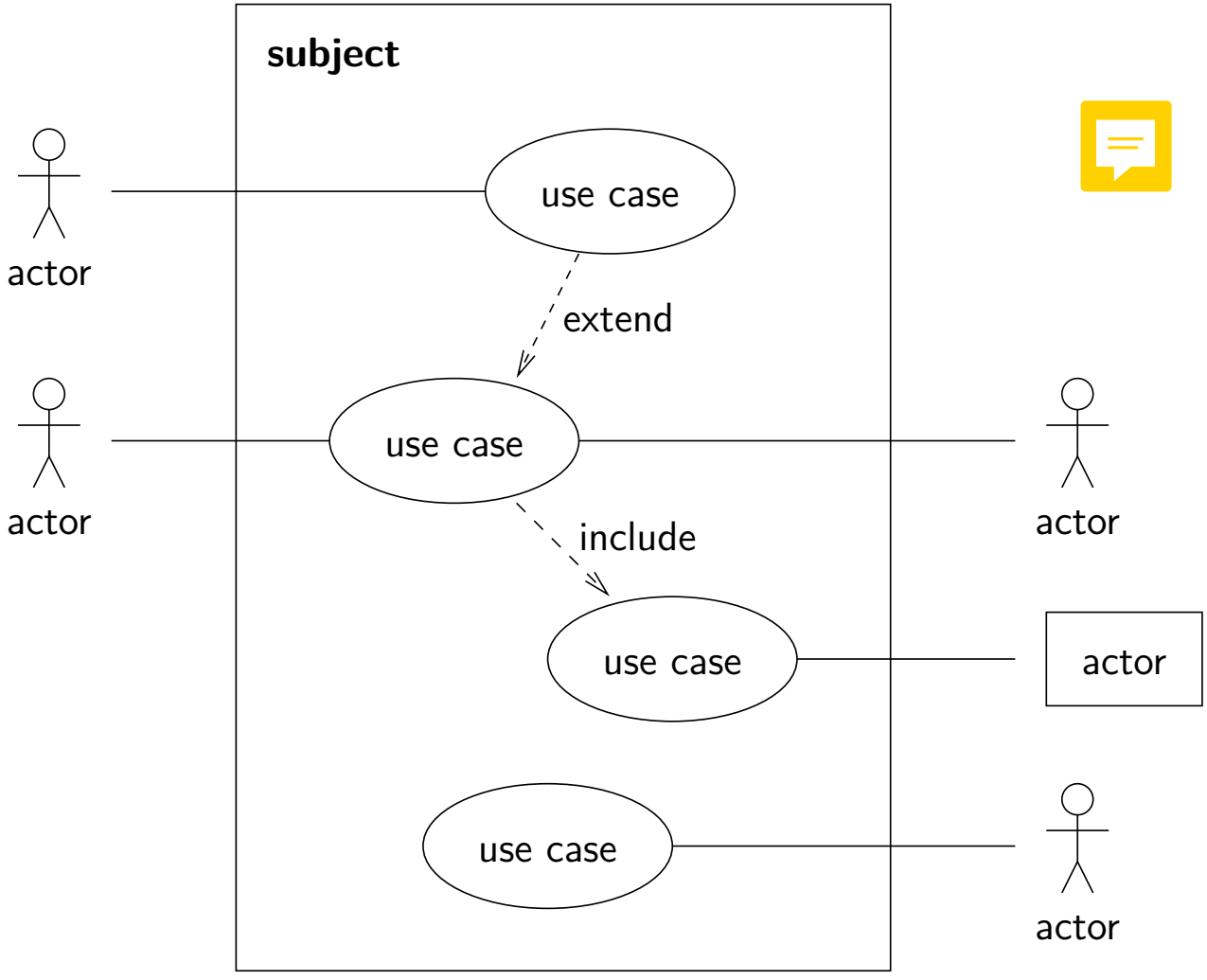


Figure 13: UML use case diagram

UML

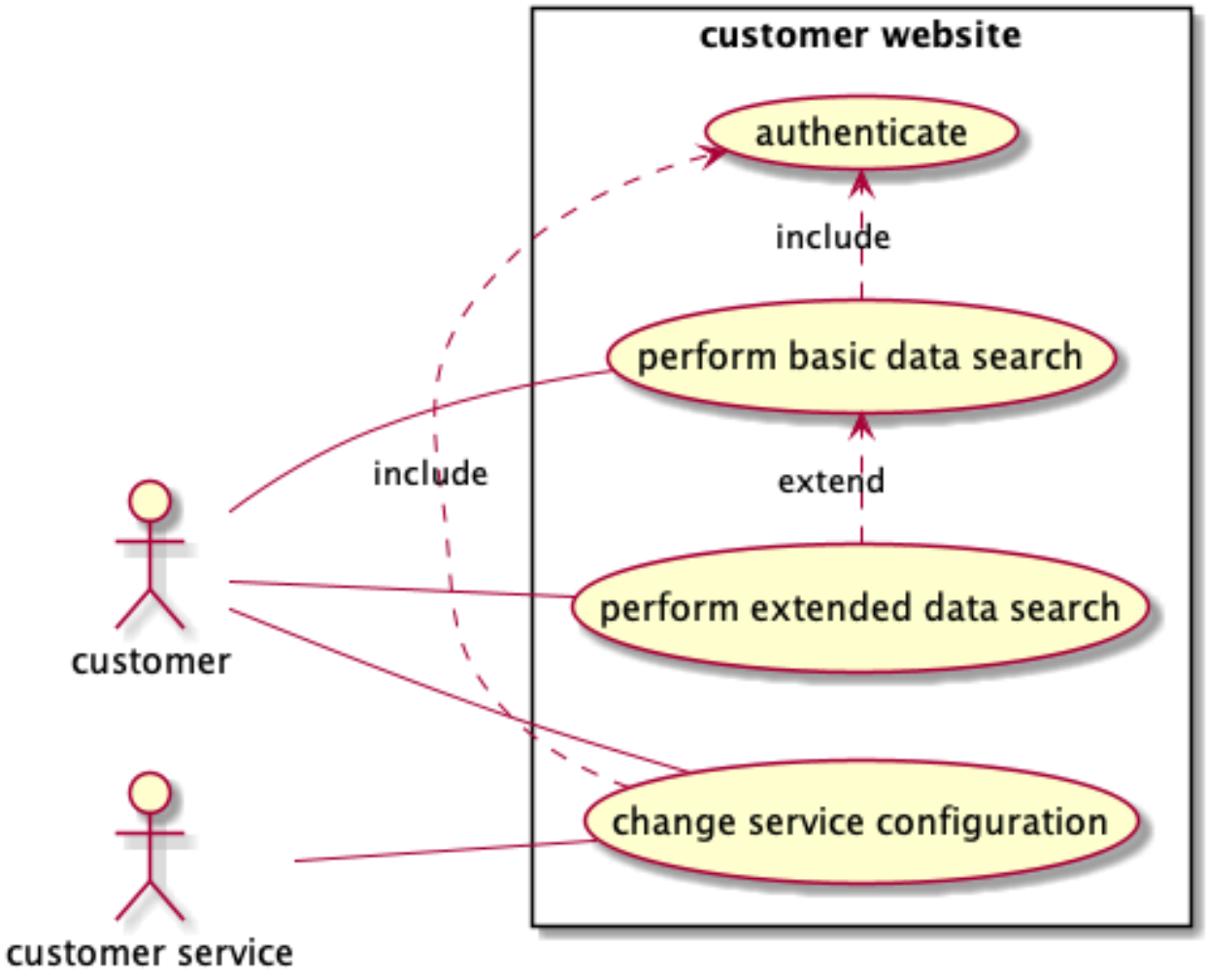


Figure 14: UML use case diagram

UML

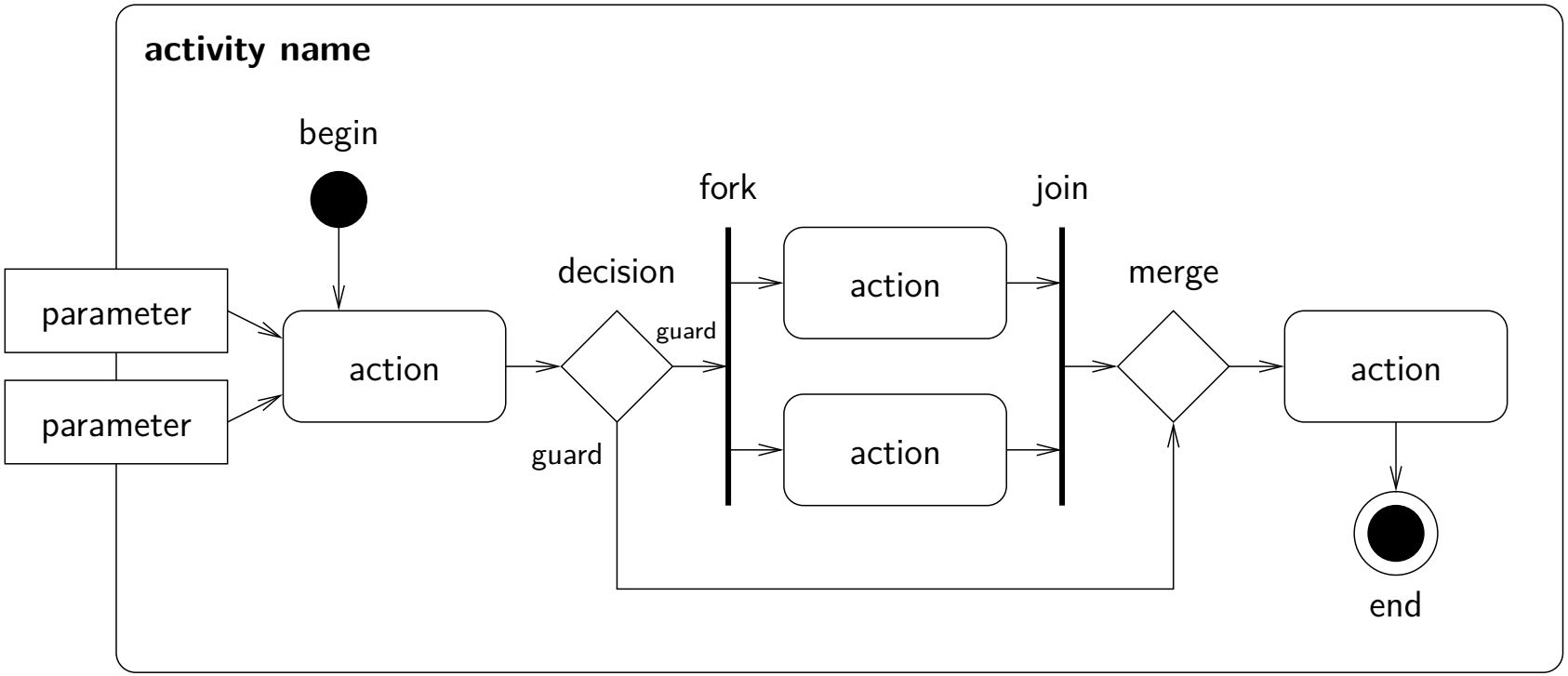


Figure 15: UML activity diagram

UML

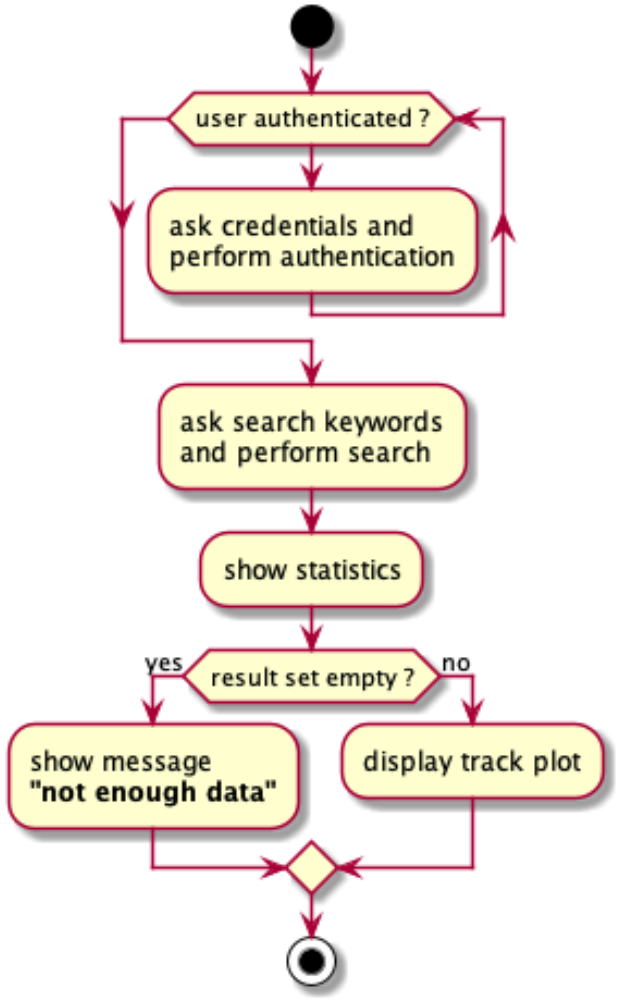


Figure 16: UML activity diagram

information systems

DFD

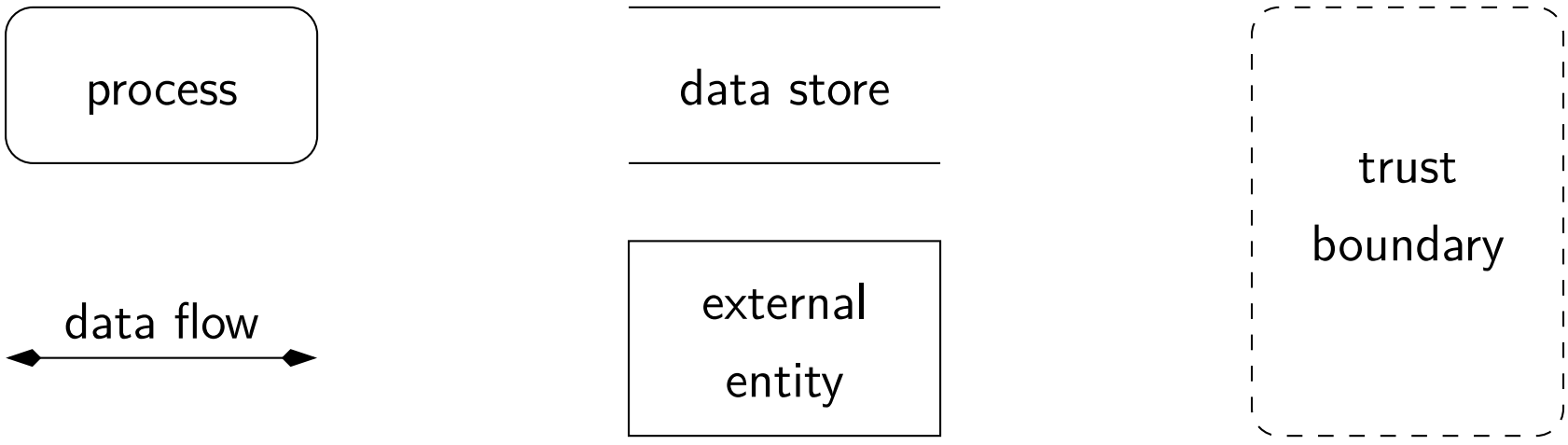


Figure 17: DFD

DFD

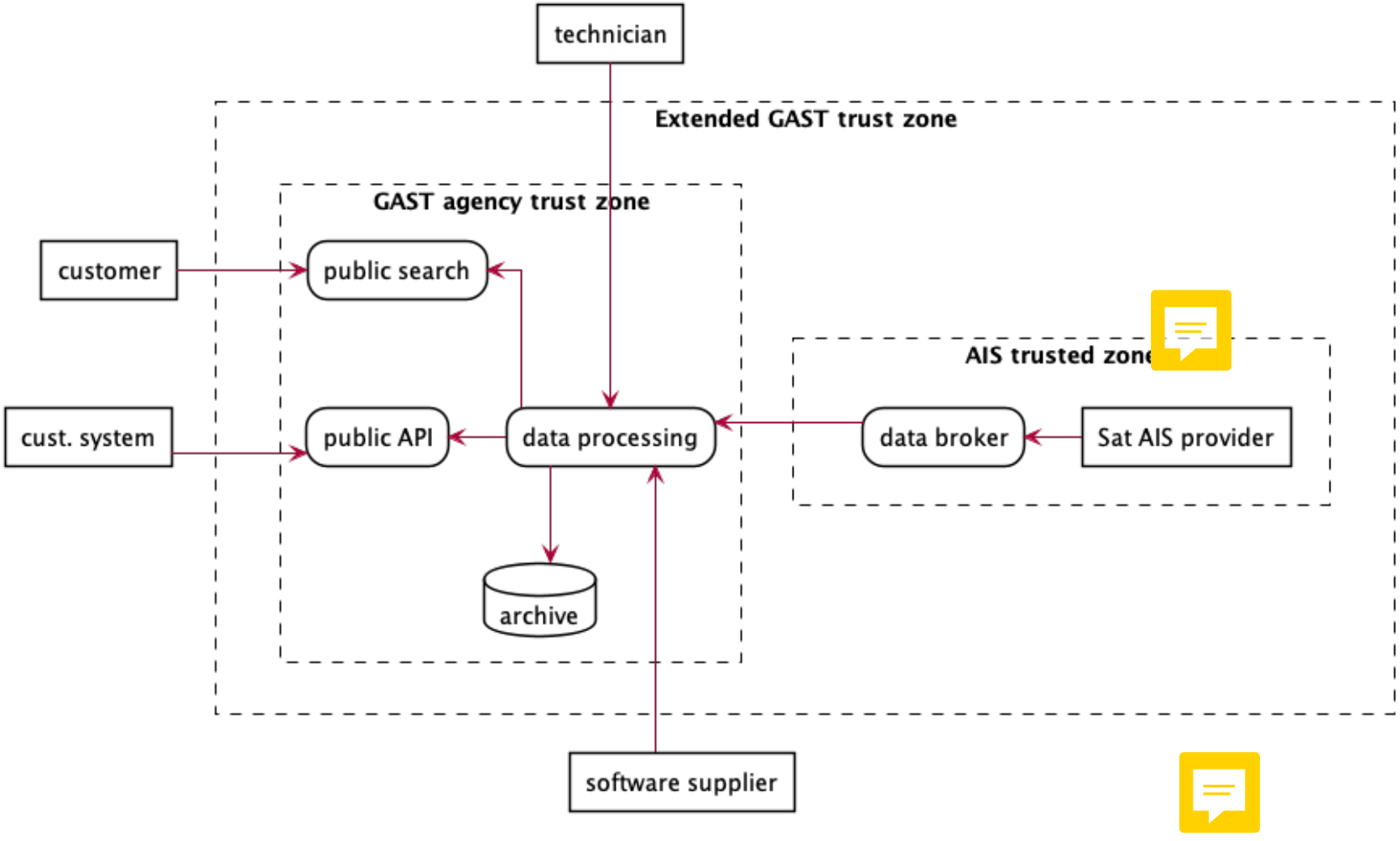


Figure 18: DFD

technology

C4

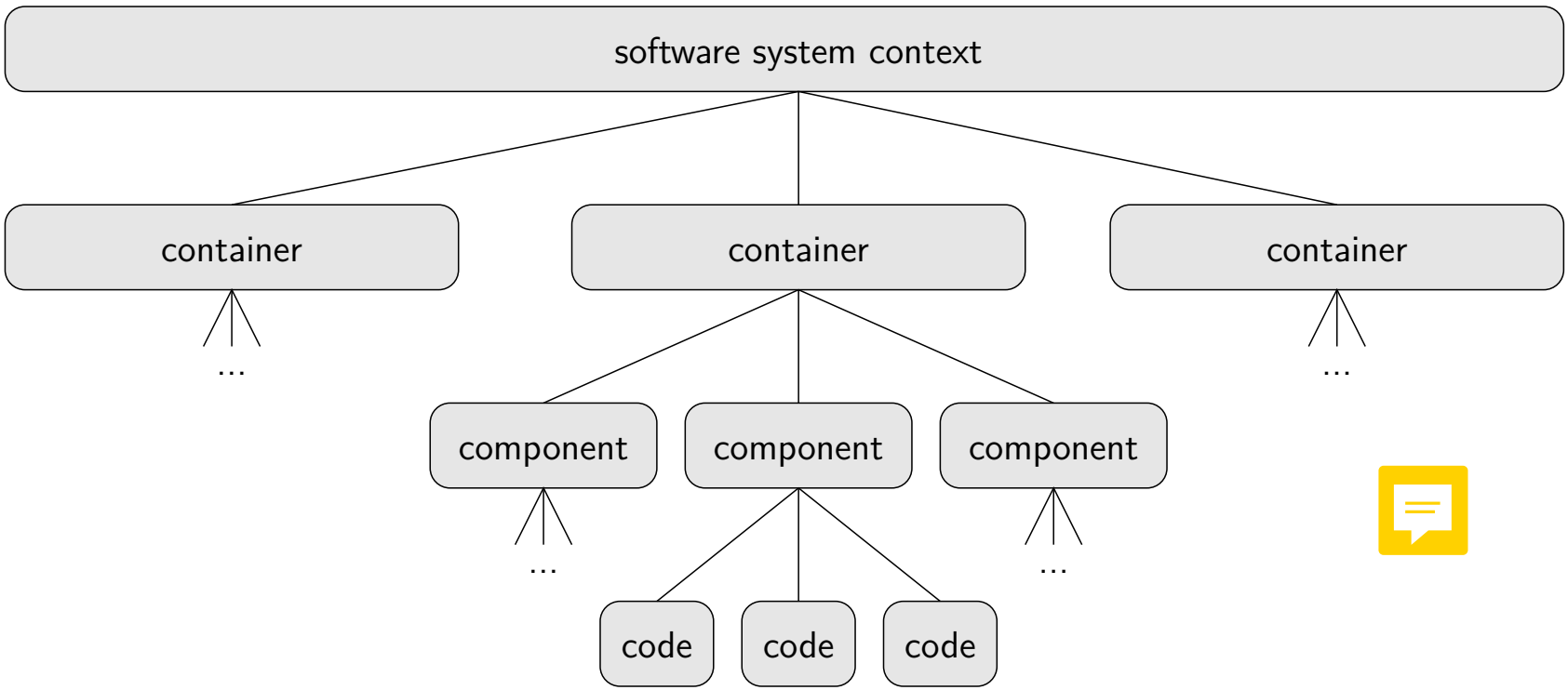


Figure 19: C4 model

C4

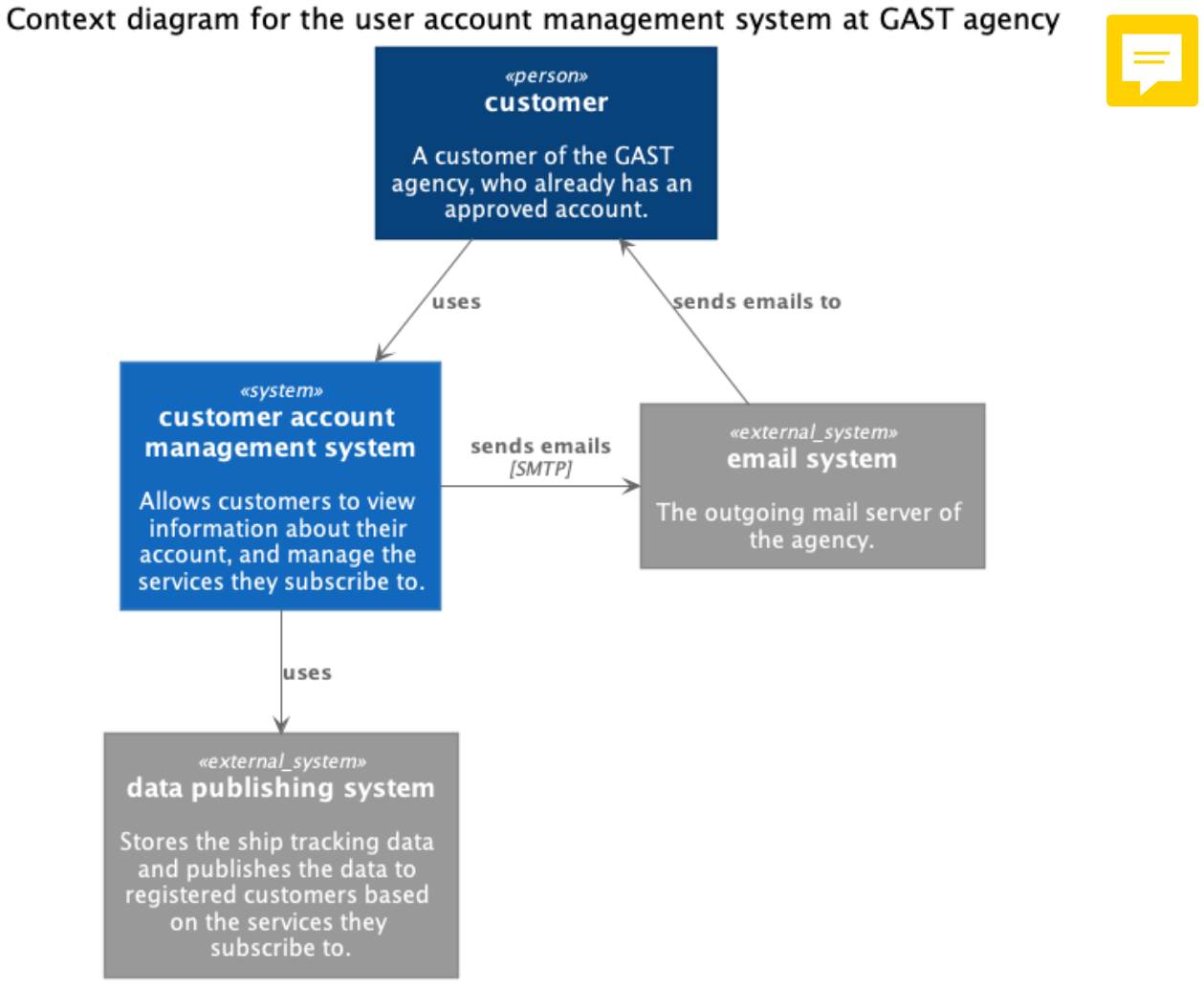


Figure 20: C4 model

C4

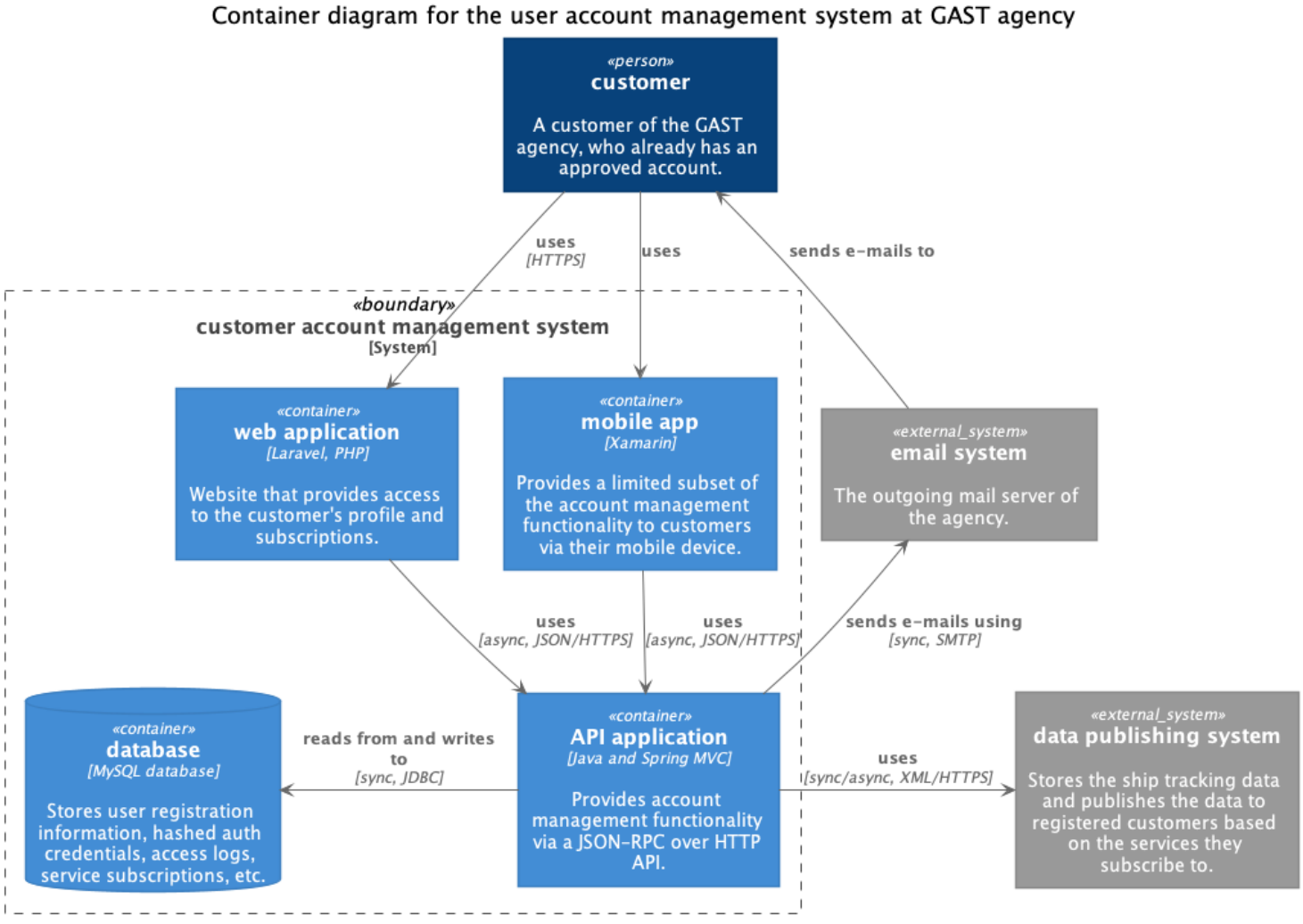


Figure 21: C4 model

C4

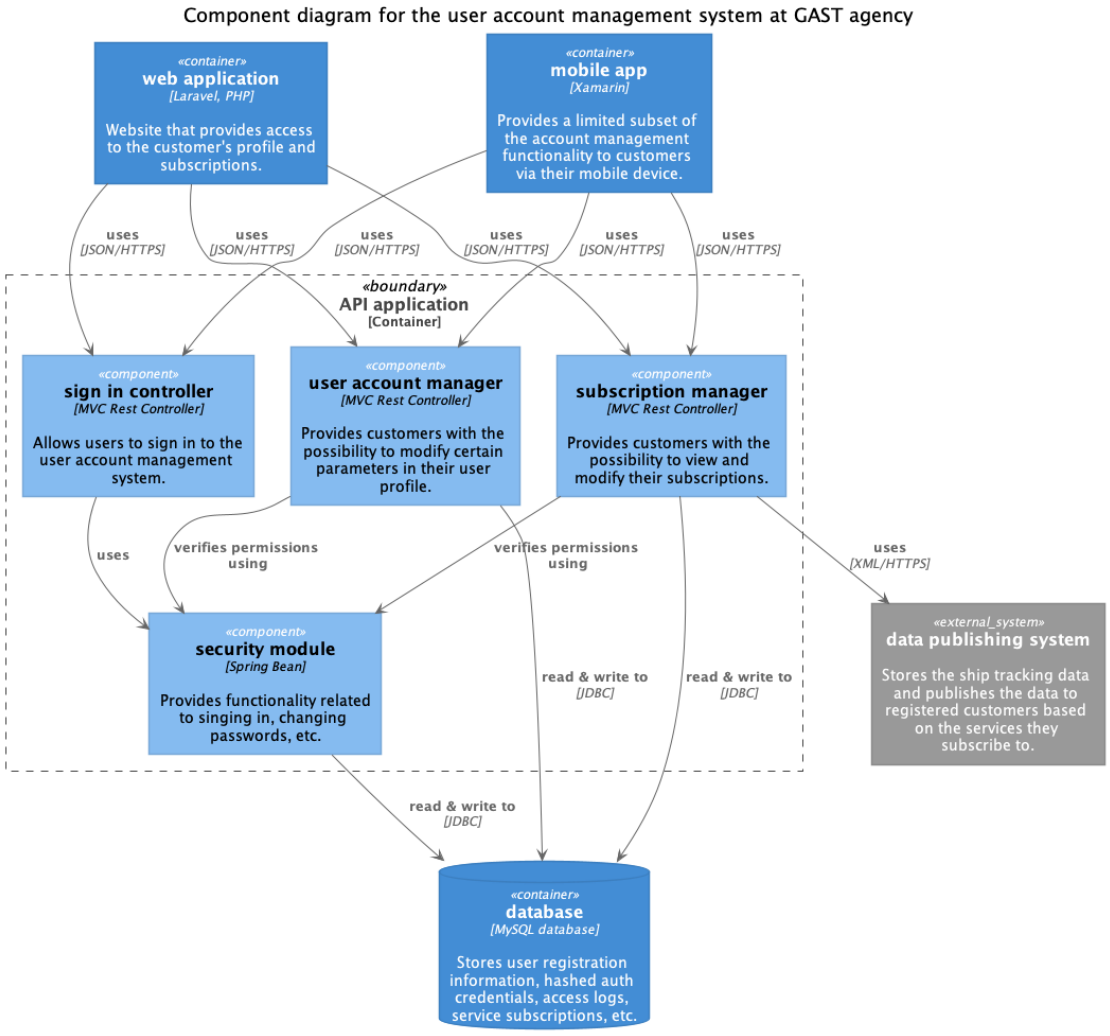


Figure 22: C4 model

any other diagram

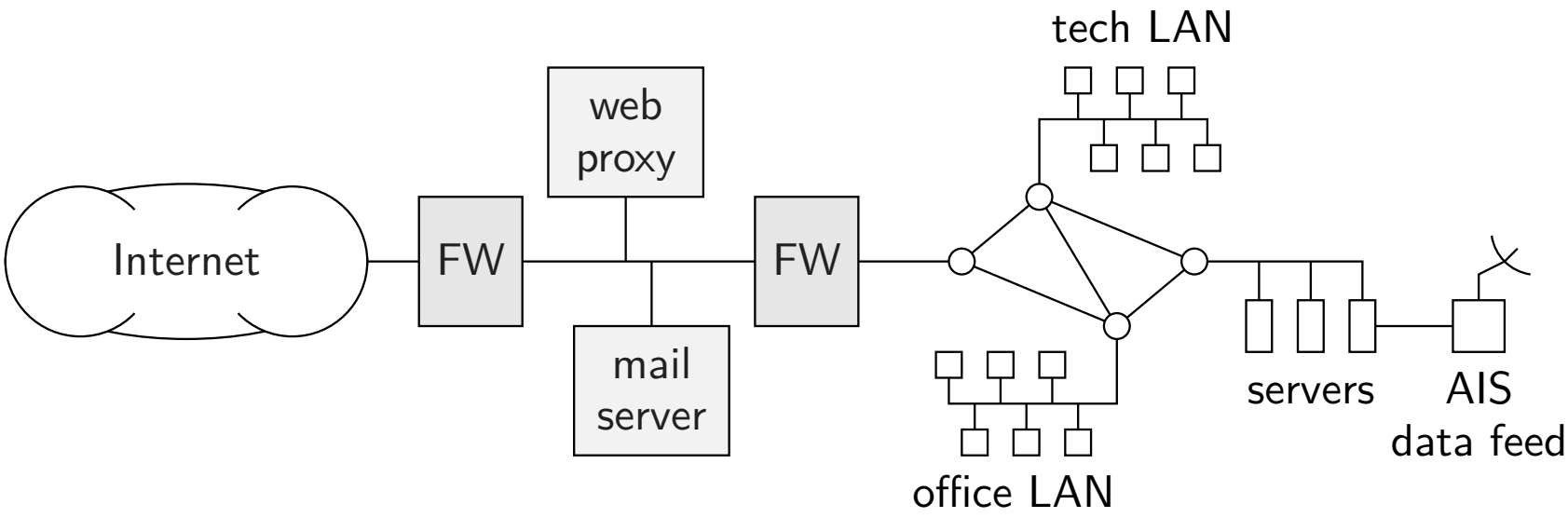


Figure 23: for instance a basic network diagram

conclusions

conclusions

Figure 24: questions or comments ?