UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Lecture 12 – Authentication, Authorization, Auditing

Prof. Esposito Christian

::.. Summary

- Authentication and Authorization
  - Identity Manager;
  - Access Control Models;
  - Kerberos, X.509, SAML, XACML, OAuth2;
  - Trust Management
- Auditing and Intrusion Detection Systems

::.. Key Lectures

- El-hajj, Mohammed, et al. "A survey of internet of things (IoT) Authentication schemes", Sensors 19(5): 1141, 2019.
- Ravidas, Sowmya , Alexios Lekidis, Federica Paci, Nicola Zannone, "Access control in Internet-of-Things: A survey", Journal of Network and Computer Applications, 144: 79-101, 2019.
- Mohammadi, V., Rahmani, A.M., Darwesh, A.M. et al. "Trust-based recommendation systems in Internet of Things: a systematic literature review", Hum. Cent. Comput. Inf. Sci. 9(21), 2019.

Authentication

::.. Introduction

(User) Authentication: The identity of users/nodes has to be validated, so as to let only certain known identities to access resources and functions.

Authorization: The rights to access certain notifications or even to use certain service functionalities are granted to given authenticated users depending on several factors, such as their role within a given organization or properly formalized security policies.

Accountability: Each activity triggered by users has to be persistently traced so as to allow later forensic analysis and to map a security threat to a responsible party.

::.. IdM (1/7)

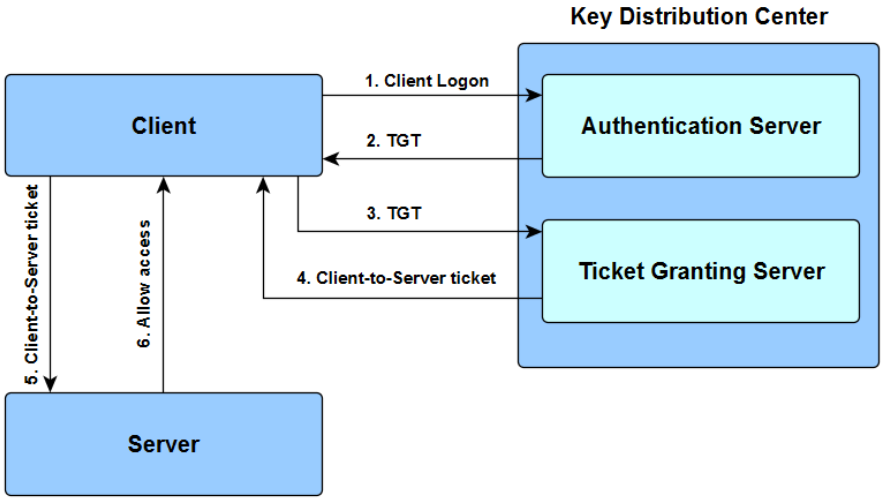
An identity is the representation of an entity in a particular context, made of a unique identifier and a set of attributes related to the user, and needs proper systems known as Identity Manager (IdM), responsible of controlling the life-cycle of identities, verifying the truthfulness of claimed identities and exchanging identity attributes with peer systems.

Over the years, several different models for representing identities and architectures to structure IdM have been proposed:

- The password-based identity models are the most simple and most commonly used: each user has a unique identifier in the system and a given password, to use to perform his/her authentication.

::.. IdM (2/7)

1. The user securely provides his/her identifier and password to IdM.
2. If the IdM finds a match between the received and the stored information, the authentication is successful and the user receives in return an access token.
3. Such a token is an opaque string that temporally identifies a user and can be used to access the services which trust the IdM releasing it.



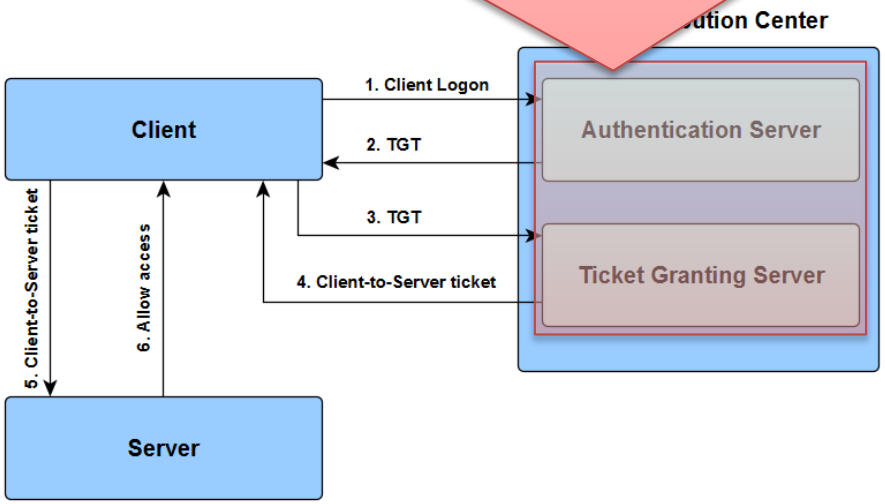
An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (2/7)

The trusted third-party authentication service includes following two servers:

- Authentication Server (AS) that performs the initial authentication and issues ticket-granting tickets (TGT) for users.
- Ticket-Granting Server (TGS) that issues service tickets that are based on the initial ticket-granting tickets (TGT).

IdM re



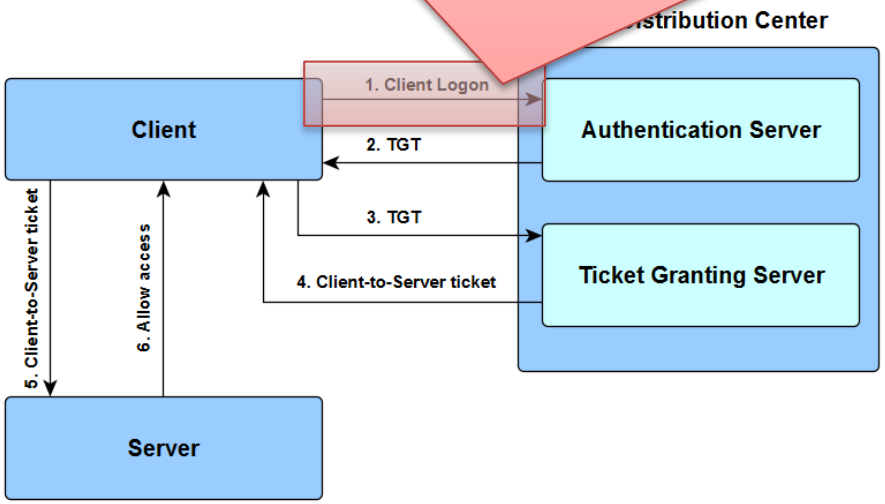
An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (2/7)

1. The user securely provides his/her identifier and password to IdM.
2. If the IdM finds a match between the received and the stored

Client sends a request to Authentication Server (AS) with plaintext user ID and asking for a server access on behalf of the user. This request is partially encrypted with a secret key which is the password of the client user.

IdM re



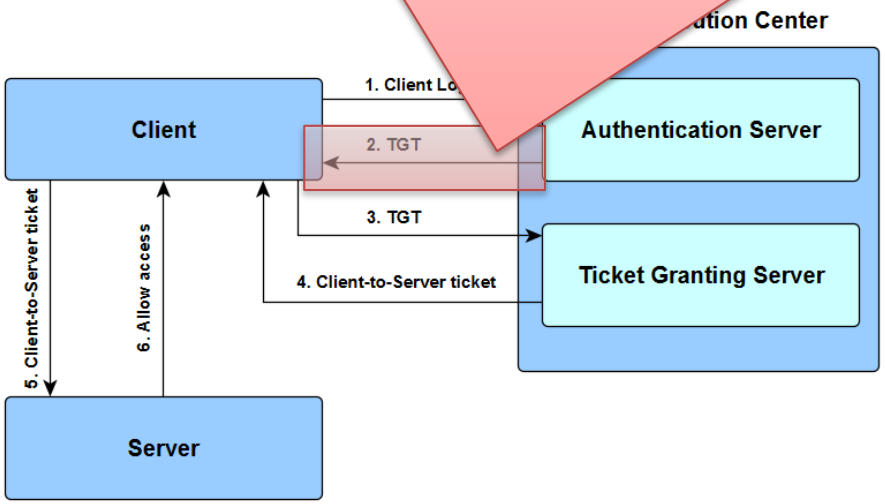
An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (2/7)

1. The user securely provides his/her identifier and password to IdM

The AS retrieve the secret key (user's password) from the user DB based on the user ID and use his password as a key to decrypt the request. That is how the user is verified. Then the AS sends a Ticket-Granting Ticket (TGT) encrypted with another secret key which is shared between AS and TGS.

IdM re



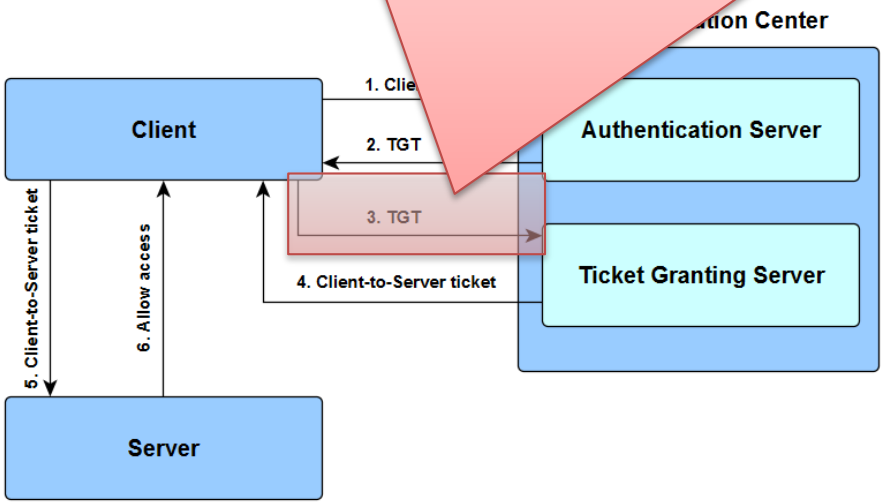
An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (2/7)

1. The user securely provides his/her identifier and password to IdM.
2. If the IdM finds a match between the received and the stored information, the authentication is successful and the user receives in return an access token.

Clients send the encrypted TGT to the TGS requesting the access for the server.

IdM r



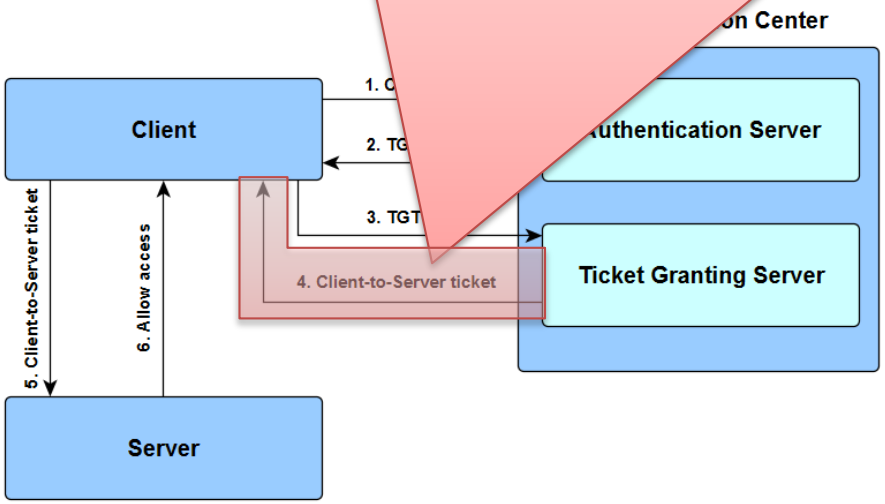
An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (2/7)

1. The user securely provides his/her identifier and password to IdM.
2. If the IdM finds a match between the received and the stored information, the authentication is successful and the user

The TGS decrypts the TGT with shared secret key with AS and issue a Kerberos token to the client which is encrypted with another shared secret key with TGS and server.

IdM r

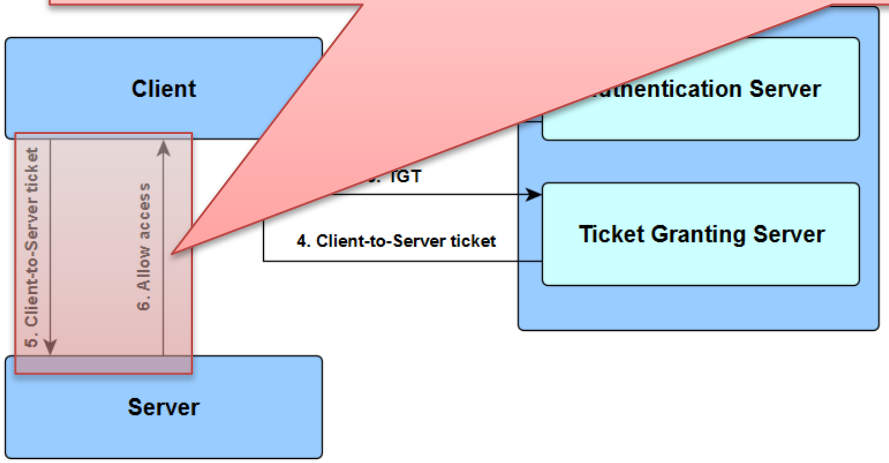


An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (2/7)

1. The user securely provides his/her identifier and password to IdM.
2. If the IdM finds a match between the received and the stored information, the authentication is successful and the user receives in return an access token.

Clients send a request to server with the encrypted Kerberos token. Then the server allow the access to the requested resources to the client for a certain period of time specified in the token.

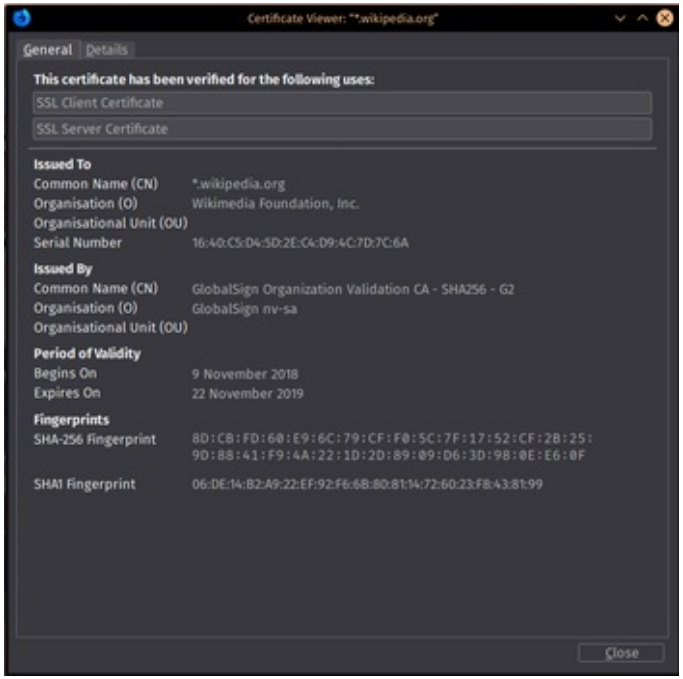


An example is Kerberos, a network authentication protocol. It is currently the default authentication technology used by Microsoft to authenticate users to services within a local area network.

::.. IdM (3/7)

Password-based authentication methods are known to be prone to vulnerabilities, depending on how “good” the used password is, e.g., how easily it can be guessed.

- A different kind of model is the one called certificate-based identity management, that makes use of digital certificates and public-key cryptography.

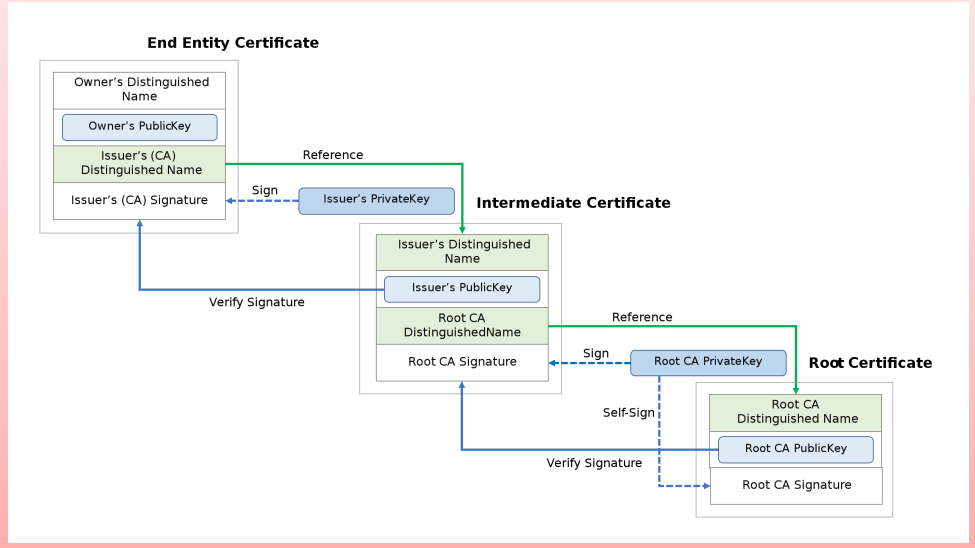


- A digital certificate is a data structure containing the user’s identifier, and his/her public key and identity attributes, verified and signed by a trusted authority, named the Certification Authority (CA), in an unforgeable format.

::.. IdM (3/7)

Password-based authentication methods are known to be prone to vulnerabilities, depending on how “good” the used password is, e.g., how easily it can be guessed.

- A different kind of model is the one called certificate-based



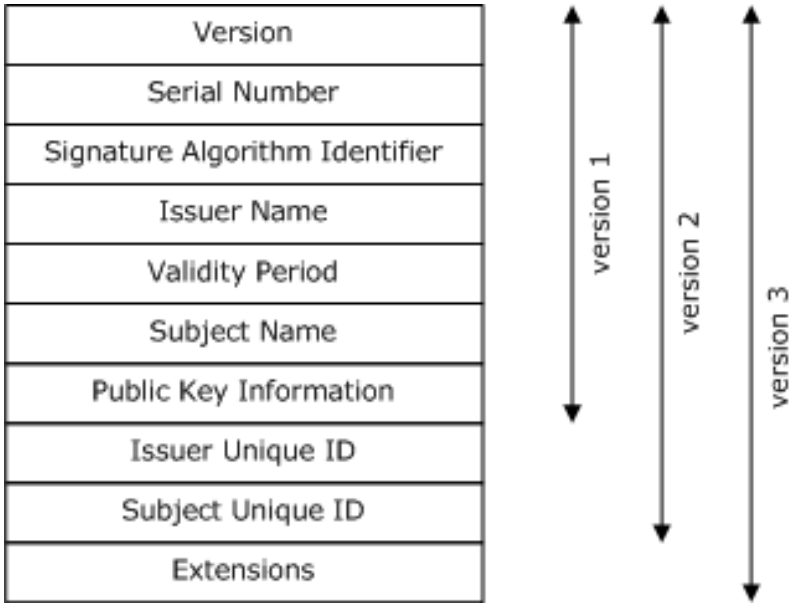
It is possible to have a hierarchy of CA so as to handle a large number of users. Each CA has its own certificate signed by the CA of higher level. Only the Root CA has a self-signed certificate.

Certification Authority (CA), in an unforgeable format.

::.. IdM (4/7)

After a user has obtained a certificate, he/she can give it to a service provider, which can verify its authenticity by interacting with the authority that has issued it. If the certificate is verified as being authentic, then the user is authenticated.

- X.509 is a standard defining the format of public key certificates and defines:



  - certificate revocation lists, to distribute information about certificates that have been deemed invalid by a signing authority,
  - certification path validation algorithm, which allows for certificates to be signed by intermediate CA certificates, which are, in turn, signed by other certificates, eventually reaching a trust anchor.

::.. IdM (4/7)

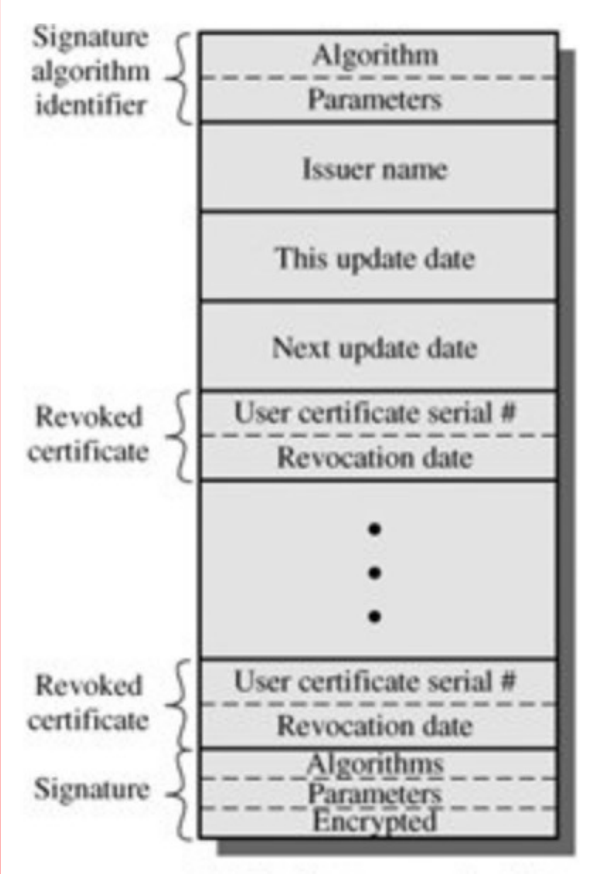
After a user has obtained a certificate, he/she can give it to a service provider, which can verify its authenticity by interacting with the authority that has issued it. If the certificate is verified as being authentic, then the user is authenticated.

- X.509 is a standard defining the format of public key certificates and defines:

```
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division,
        CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    Validity
      Not Before: Jul  9 16:04:02 1998 GMT
      Not After : Jul  9 16:04:02 1999 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
        OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb: 33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
          66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66: 70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
          16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b: c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
          8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3: d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
          e8:35:1c:9e:27:52:7e:41:8f
        Exponent: 65537 (0x10001)
  Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
    ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67: d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
    0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1: 5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
    8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:68:9f
```

  - certificate revocation lists, to distribute information about certificates that have been deemed invalid by a signing authority,
  - certification path validation algorithm, which allows for certificates to be signed by intermediate CA certificates, which are, in turn, signed by other certificates, eventually reaching a trust anchor.

::.. IdM (4/7)



The standard also specifies the format of the certificate revocation lists.

certificate, he/she can give it to a
erify its authenticity by interacting
ued it. If the certificate is verified
r is authenticated.

ing the format of public key

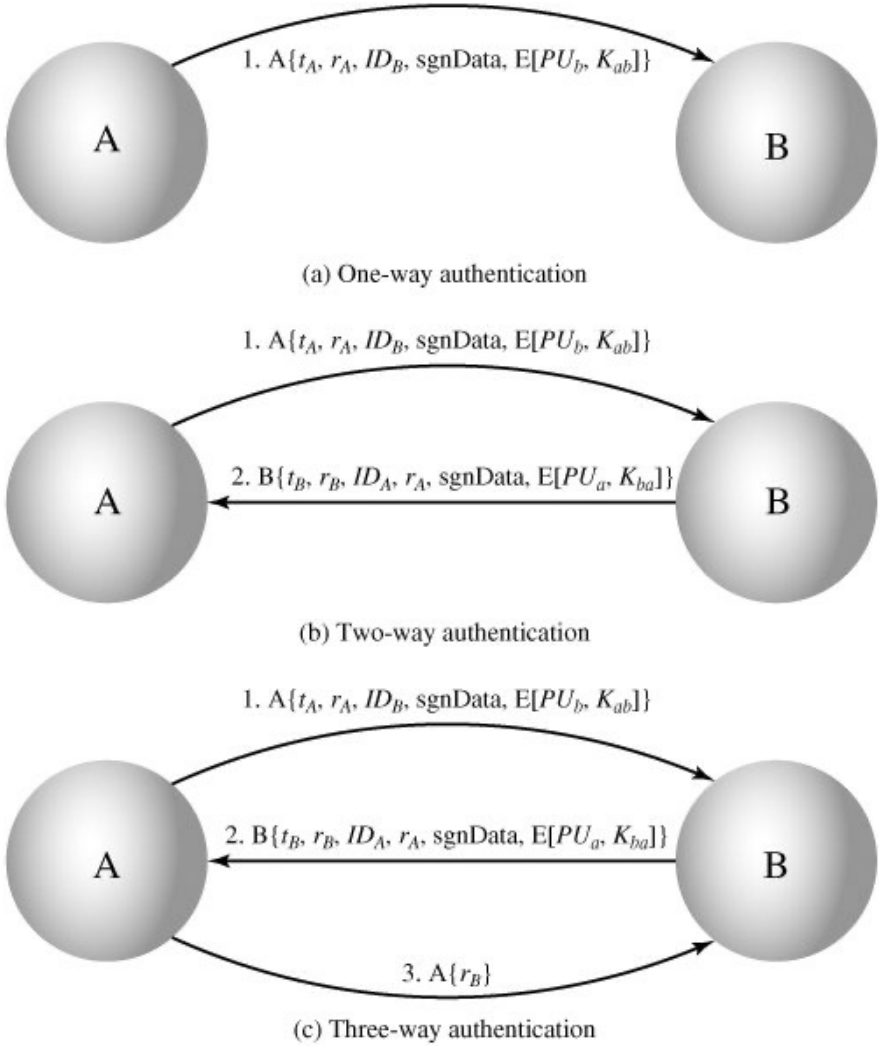
certificate revocation lists, to distribute information about certificates that have been deemed invalid by a signing authority,

certification path validation algorithm, which allows for certificates to be signed by intermediate CA certificates, which are, in turn, signed by other certificates, eventually reaching a trust anchor.

93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67: d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1: 5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:68:9f

::.. IdM (5/7)

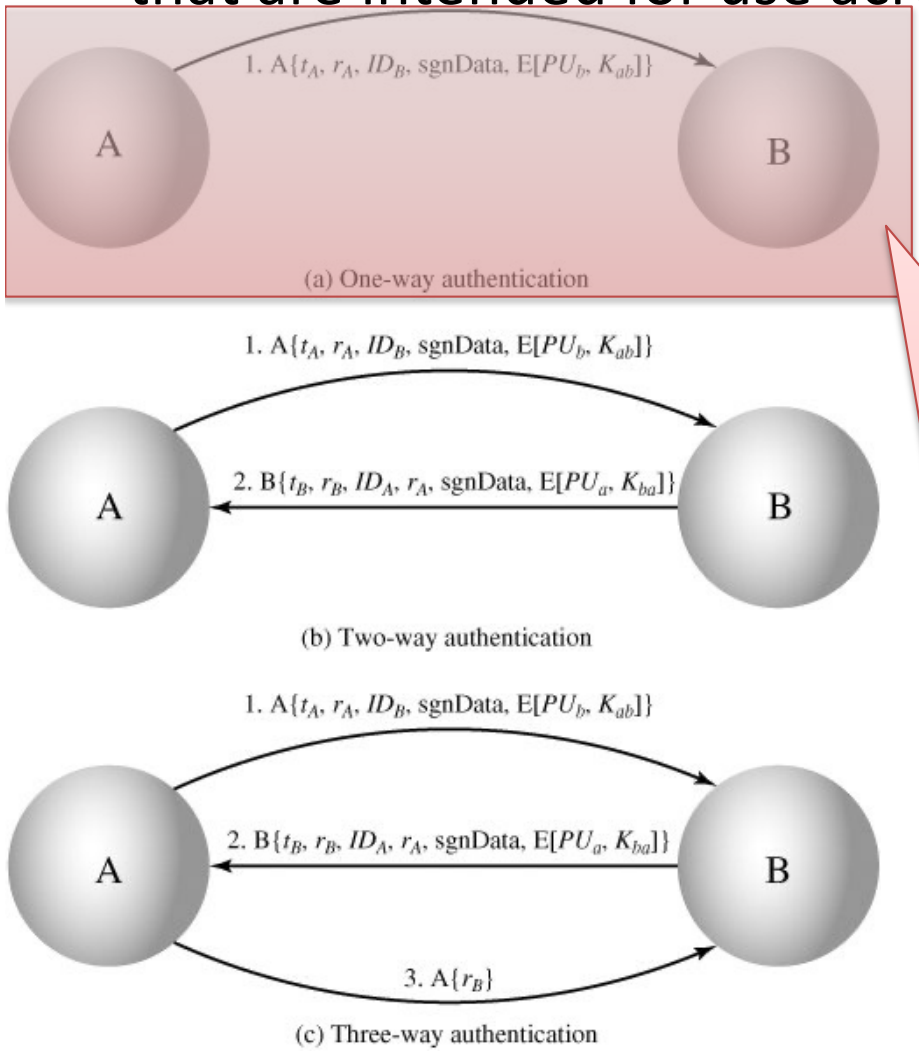
X.509 also includes three alternative authentication procedures that are intended for use across a variety of applications.



It is assumed that the two parties know each other's public key, either by obtaining each other's certificates from the directory or because the certificate is included in the initial message from each side.

::.. IdM (5/7)

X.509 also includes three alternative authentication procedures that are intended for use across a variety of applications.



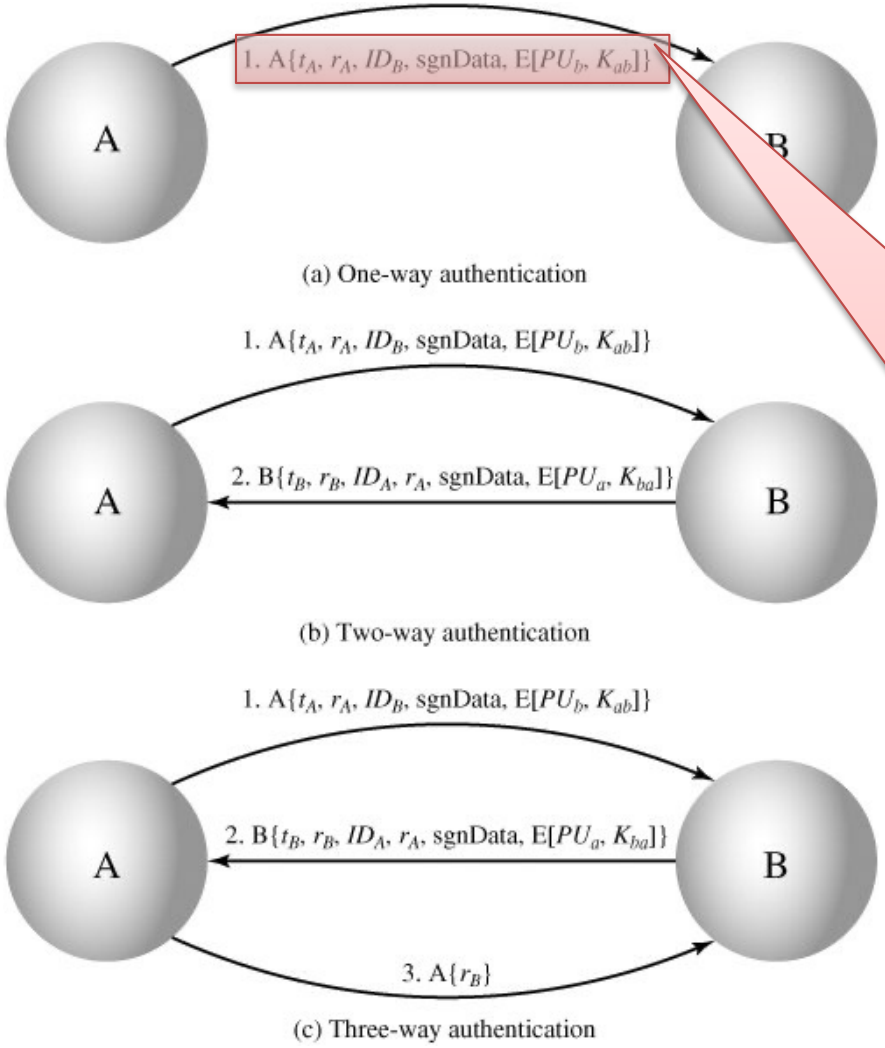
It is assumed that the two parties

One way authentication involves a single transfer of information from one user (A) to another (B), and establishes the following:

1. The identity of A and that the message was generated by A;
2. That the message was intended for B;
3. The integrity and originality (it has not been sent multiple times) of the message.

::.. IdM (5/7)

X.509 also includes three alternative authentication procedures that are intended for use across a variety of applications.

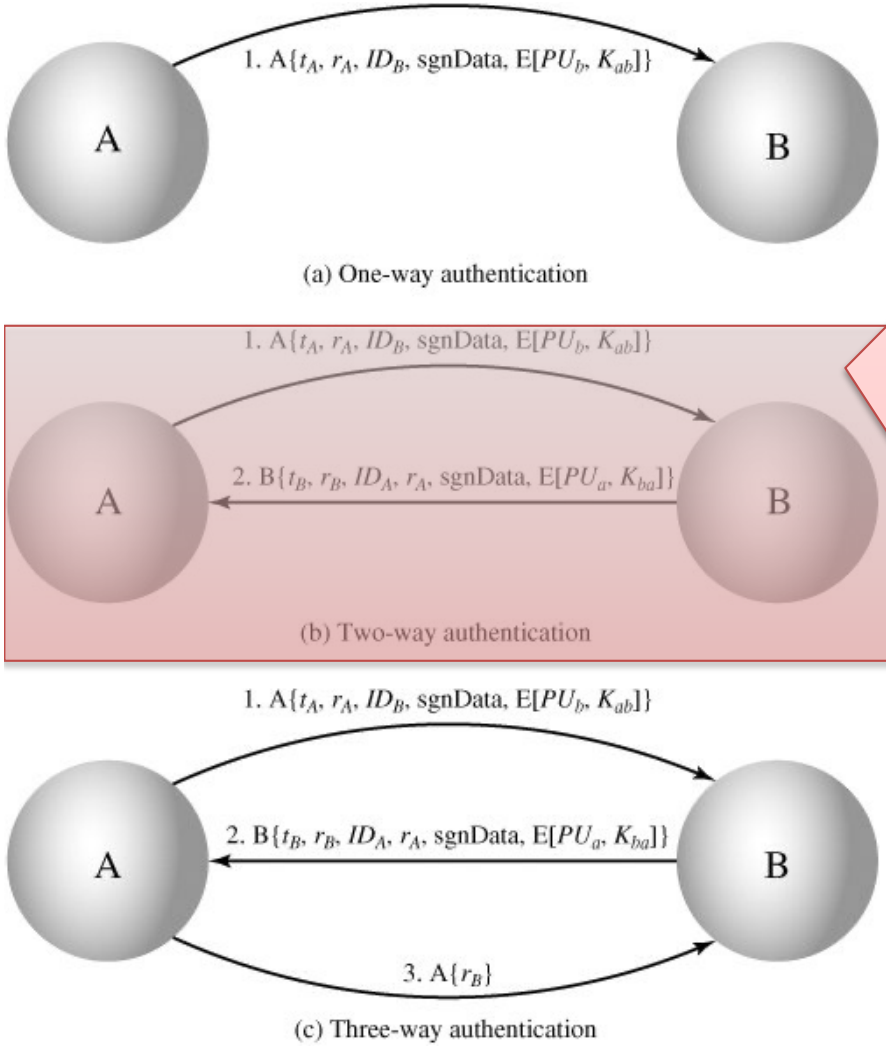


It is assumed that the two parties know each other's public key, either by obtaining each other's certificates from the directory or because the certificate is included in the initial message from each side.

The message includes a timestamp t_A, a nonce r_A and the identity of B and is signed with A's private key.

::.. IdM (5/7)

X.509 also includes three alternative authentication procedures that are intended for use across a variety of applications.



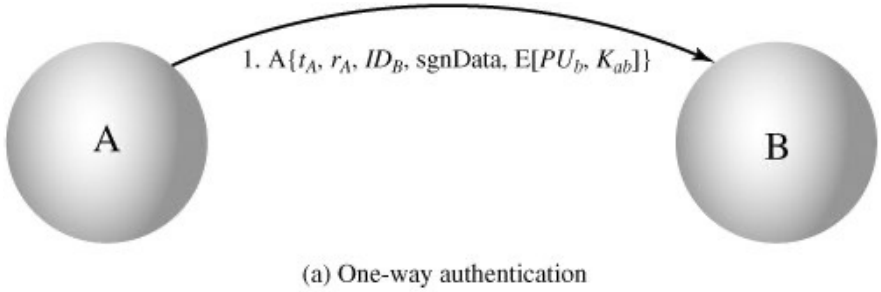
It is assumed that the two parties

1. The identity of B and that the reply message was generated by B;
2. That the message was intended for A;
3. The integrity and originality of the reply.

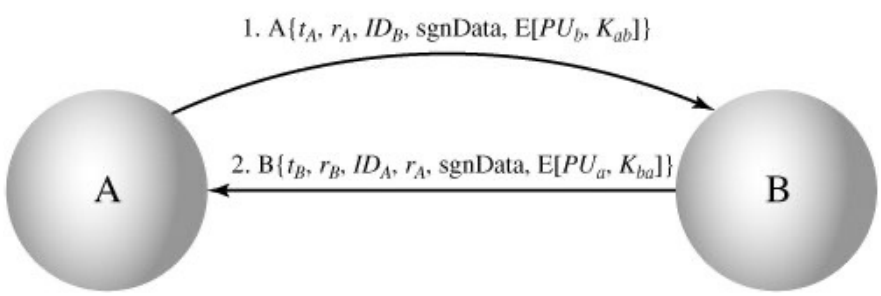
Two-way authentication thus permits both parties in a communication to verify the identity of the other.

::.. IdM (5/7)

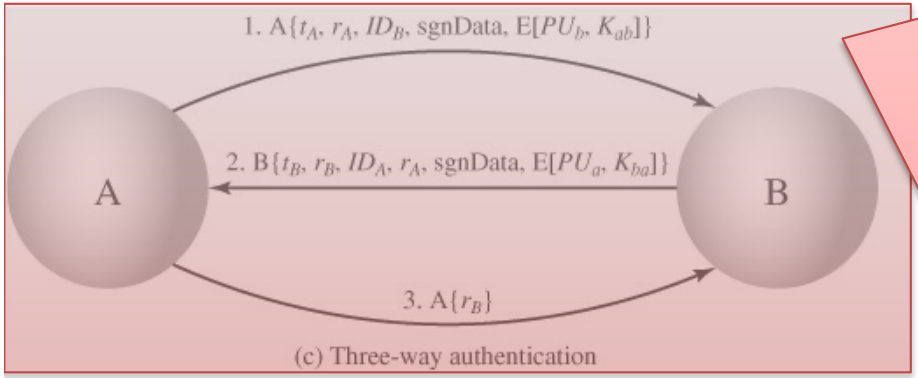
X.509 also includes three alternative authentication procedures that are intended for use across a variety of applications.



(a) One-way authentication



(b) Two-way authentication



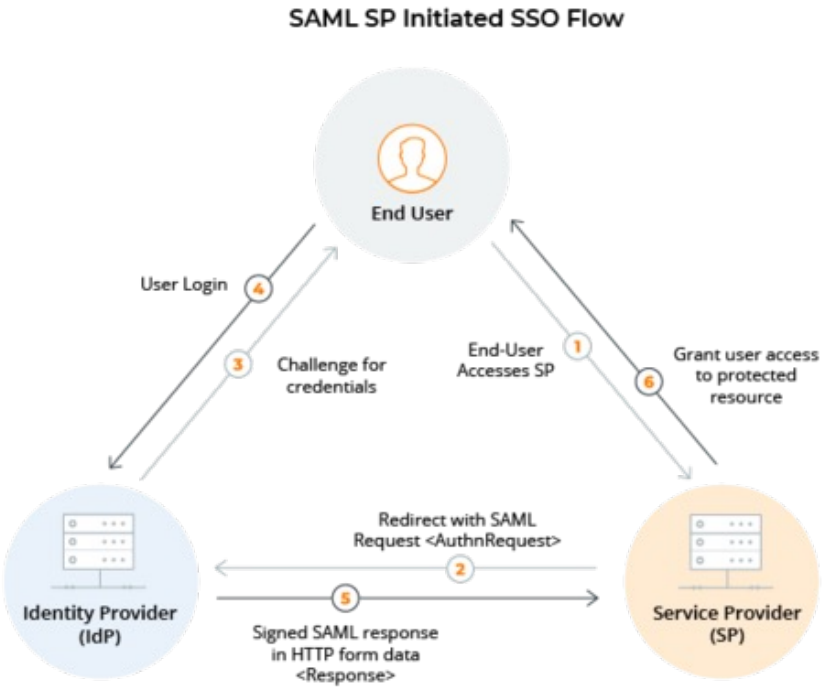
(c) Three-way authentication

It is assumed that the two parties know each other's public key, either

In three-way authentication, a final message from A to B is included, which contains a signed copy of the nonce r_B. Because both nonces are echoed back by the other side, each side can check the returned nonce to detect replay attacks. This approach is needed when synchronized clocks are not available.

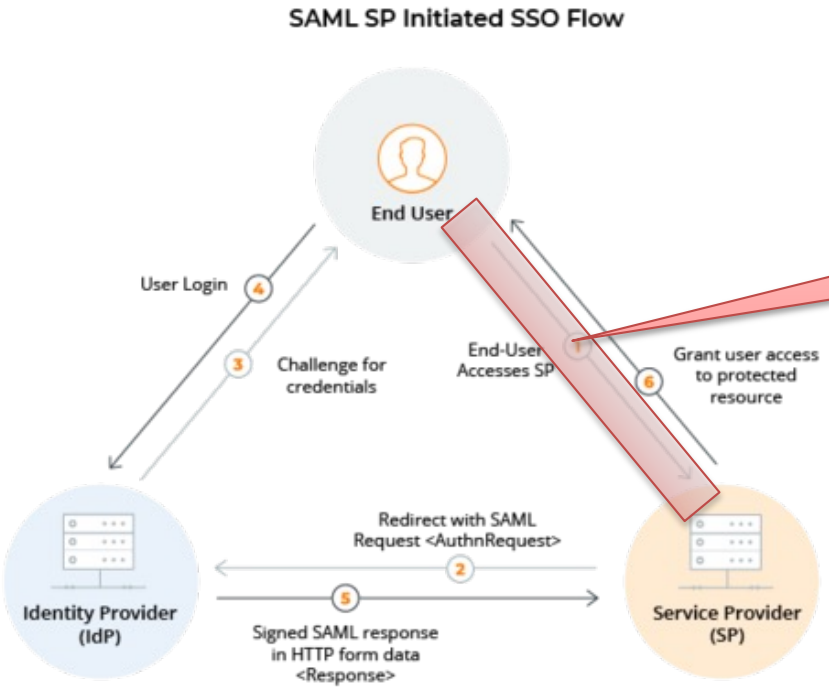
::.. IdM (6/7)

- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.



::.. IdM (6/7)

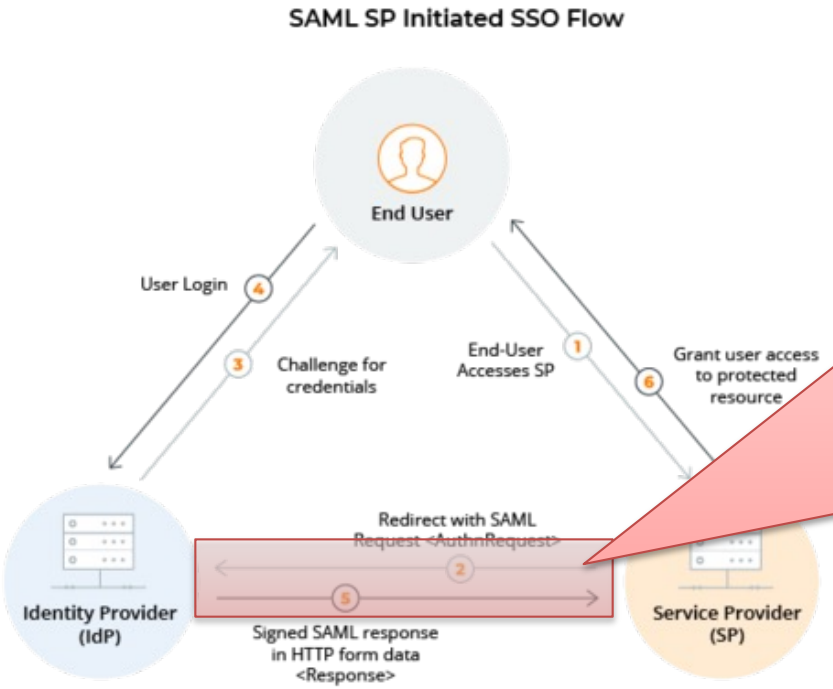
- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.



The end-user initiates the login process at the Service Providers (SP).

::.. IdM (6/7)

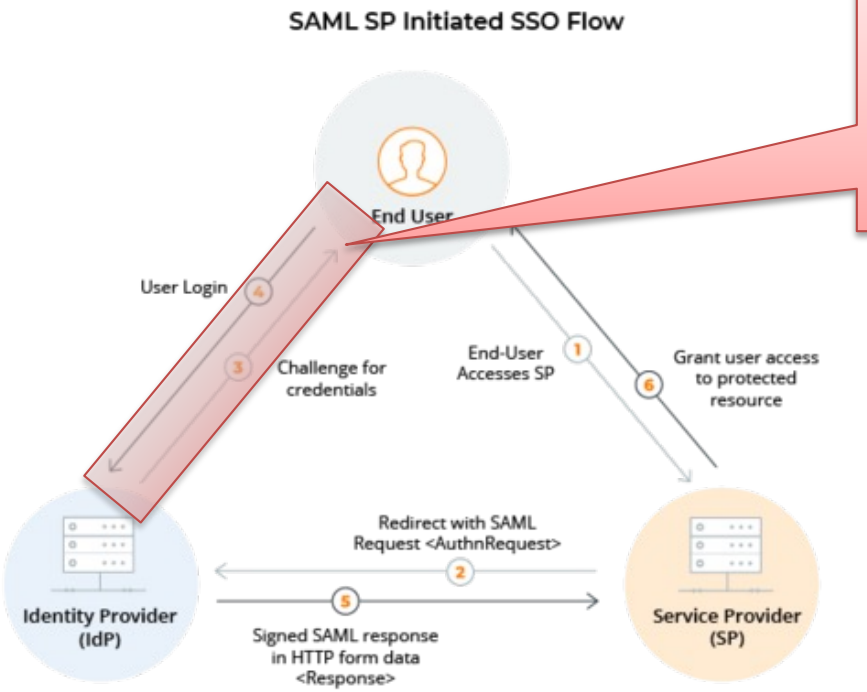
- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.



The SP will redirect the user to the IdP with a SAML Request (AuthnRequest). The SAML Request will contain the necessary information for the IdP to authenticate the end-user and reply to the SP with the correct SAML Assertion (SAMLResponse).

::.. IdM (6/7)

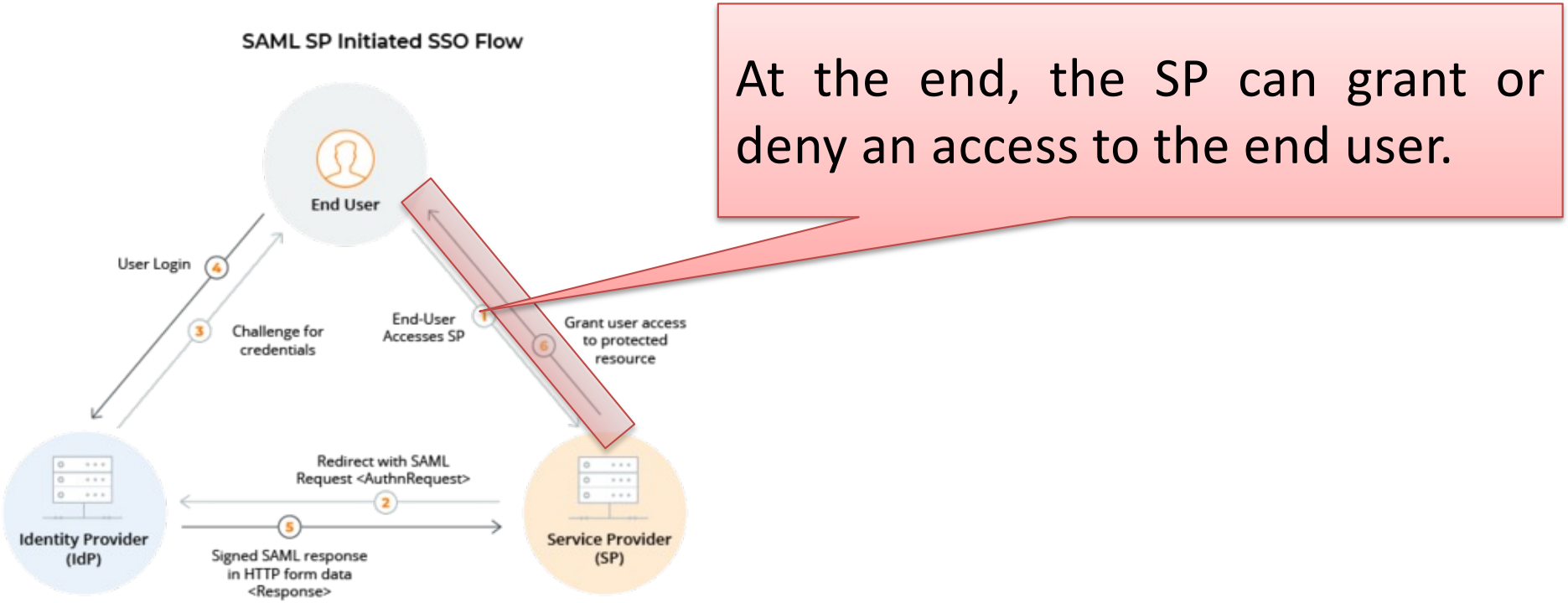
- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.



The IdM can challenge the end user so as to complete the login phase.

::.. IdM (6/7)

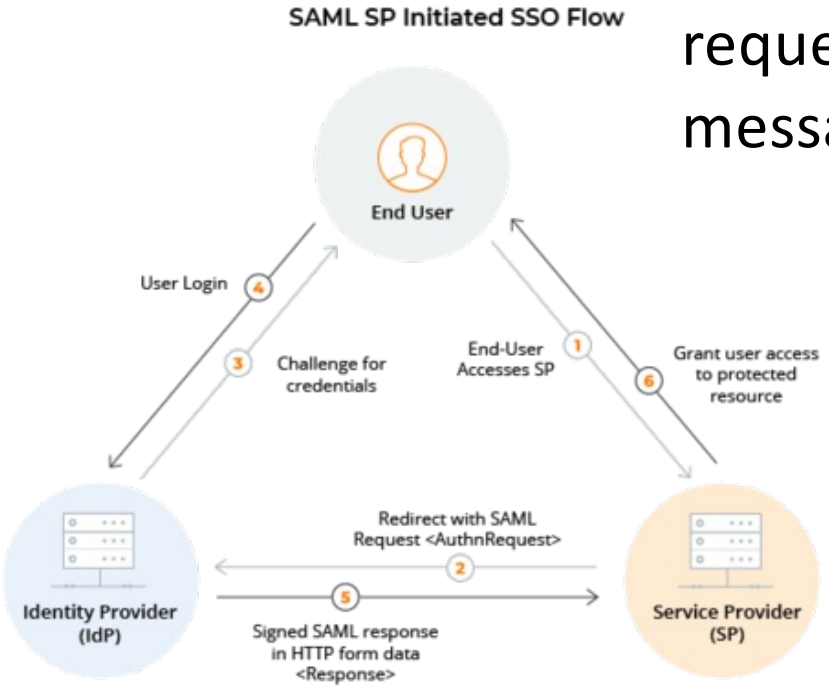
- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.

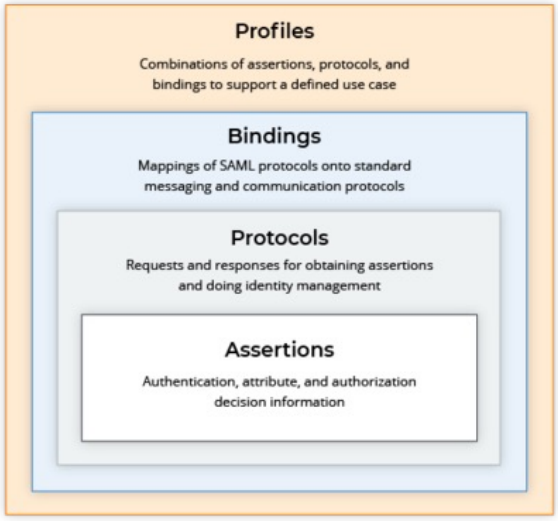


::.. IdM (6/7)

- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.

SAML's standards provide a request/response for exchanging XML messages between these roles.

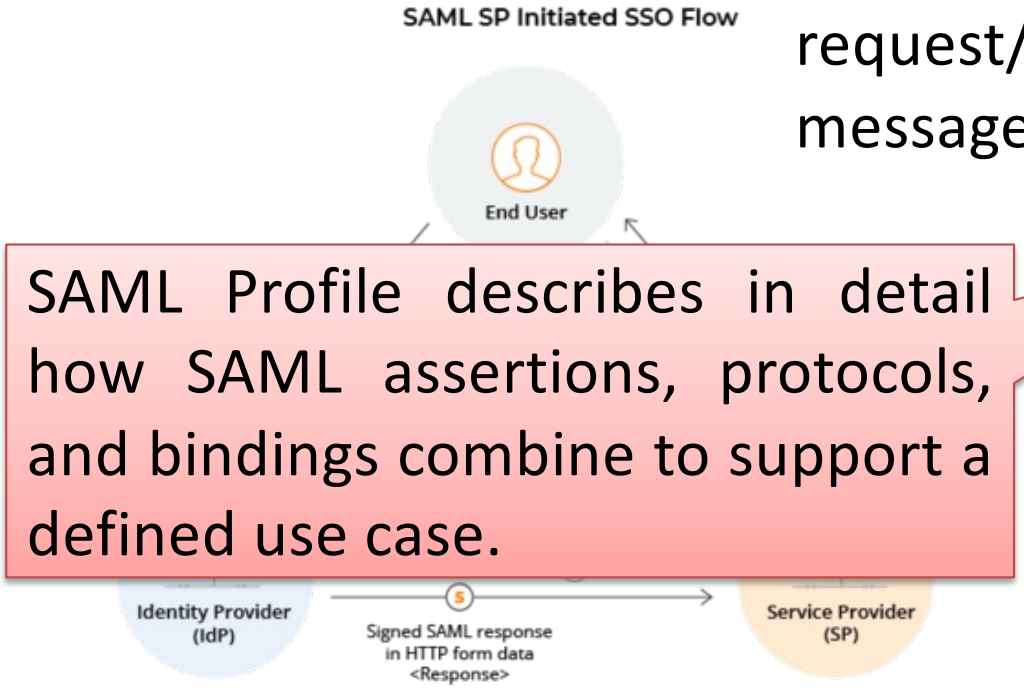




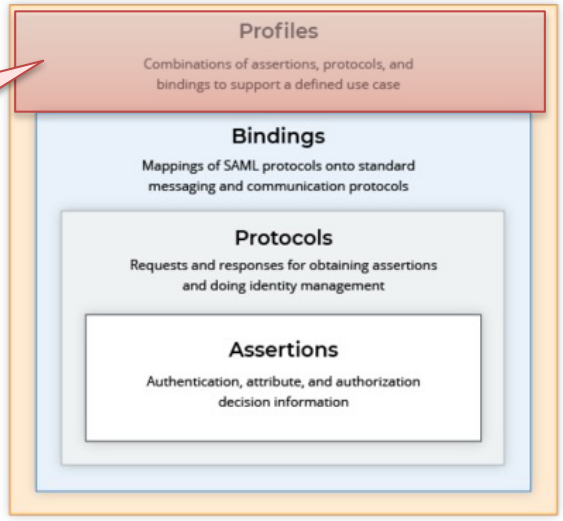
::.. IdM (6/7)

- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.

SAML's standards provide a request/response for exchanging XML messages between these roles.



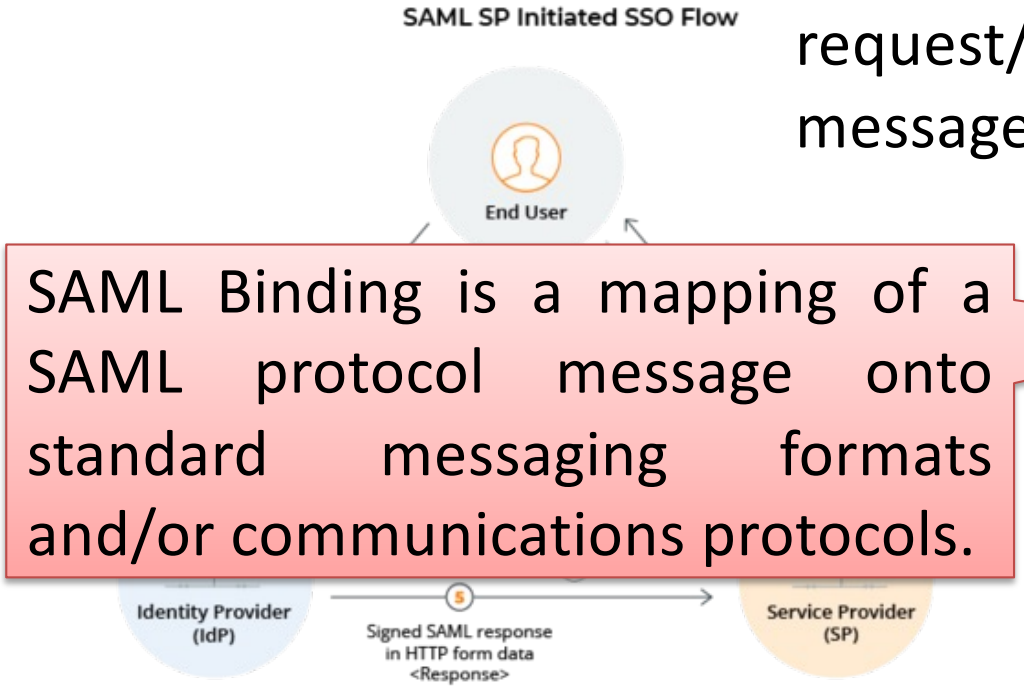
SAML Profile describes in detail how SAML assertions, protocols, and bindings combine to support a defined use case.



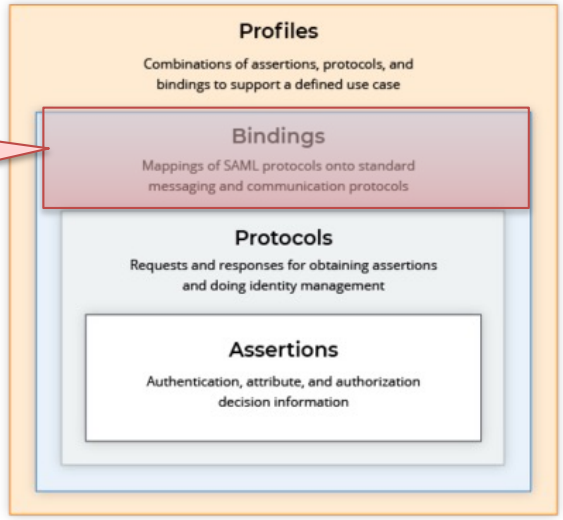
::.. IdM (6/7)

- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.

SAML's standards provide a request/response for exchanging XML messages between these roles.



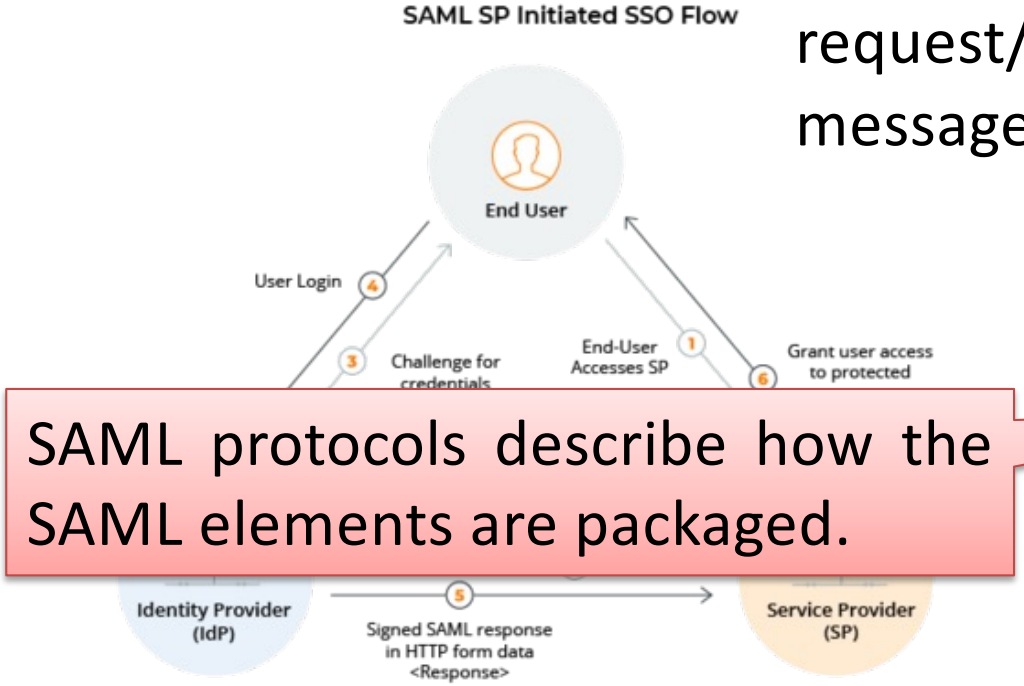
SAML Binding is a mapping of a SAML protocol message onto standard messaging formats and/or communications protocols.



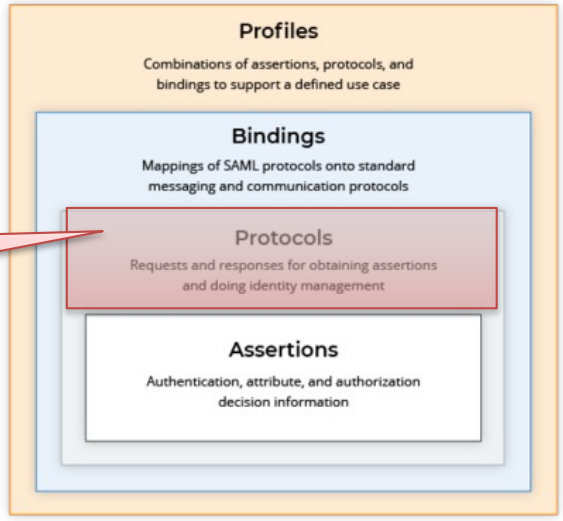
::.. IdM (6/7)

- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.

SAML's standards provide a request/response for exchanging XML messages between these roles.



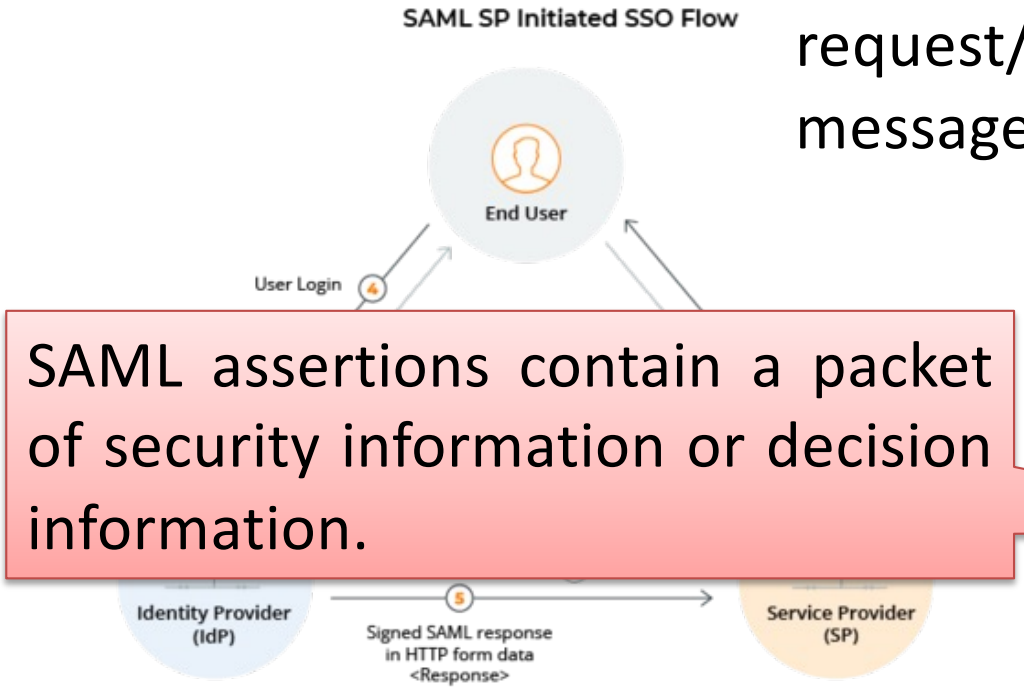
SAML protocols describe how the SAML elements are packaged.



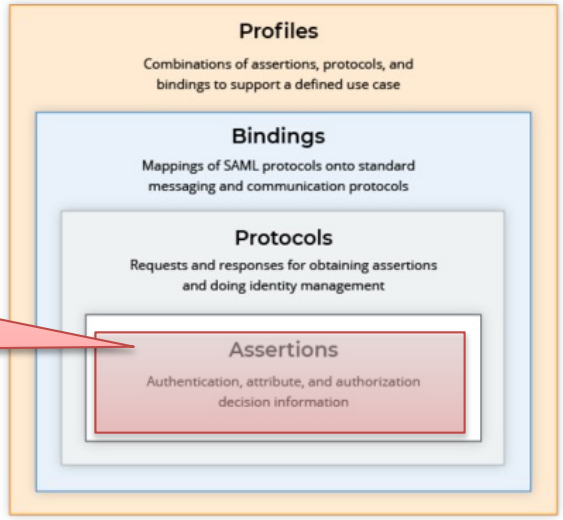
::.. IdM (6/7)

- Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider, and and XML-based markup language for security assertions.

SAML's standards provide a request/response for exchanging XML messages between these roles.



SAML assertions contain a packet of security information or decision information.



::.. IdM (7/7)

Despite offering good levels of security, such certificate-based solutions may prove to be very expensive and cumbersome.

IdM can have three possible architectures:

1. Isolated, where the service provider also acts as IdM;
2. Centralised, where a single IdM is present to manage identities for a set of service providers within a given domain;
3. Federated, where several IdMs are used within a federated trust domain so that the identities from different domains (i.e., those issued by different IdMs) are recognized over all the domains so as to realize the Single-Sign-On (SSO).

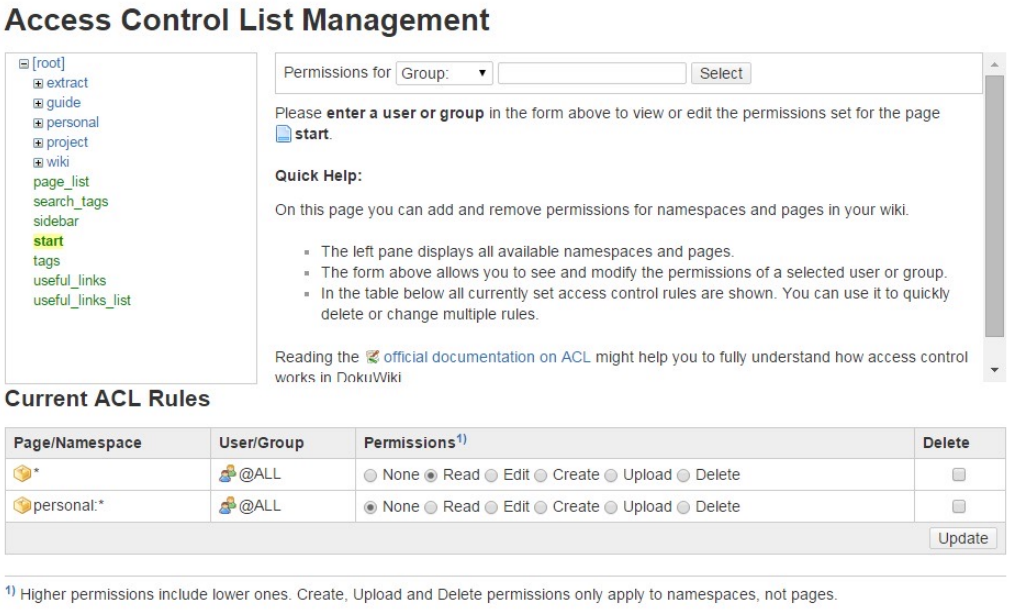
The first architecture is simple to realize, but not so scalable. The second architecture allows the management of more services with a single identity, but the centralized IdM represents a single-point-of-failure and a performance bottleneck. The last solution is more scalable and efficient, but is more complex to be realized.

Access Control

::.. Access Control (1/5)

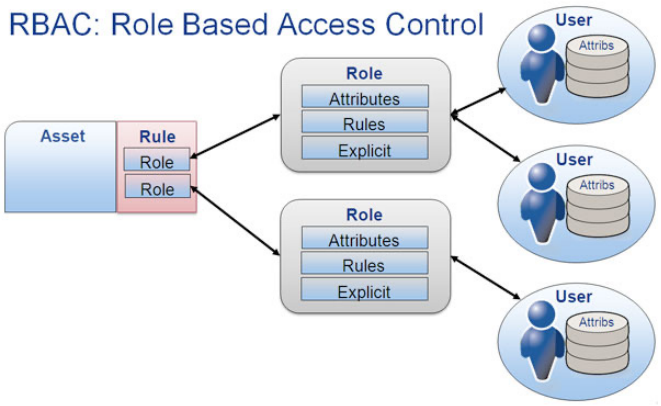
Access Control disciplines which resources of the IoT a given node is authorized to access, so as to implement authorization.

- The most basic method is known as Access Control List (ACL), sometimes known in the literature as Identity-Based Access Control (IBAC), consisting in a list of permissions attached to a resource of the system to be protected.



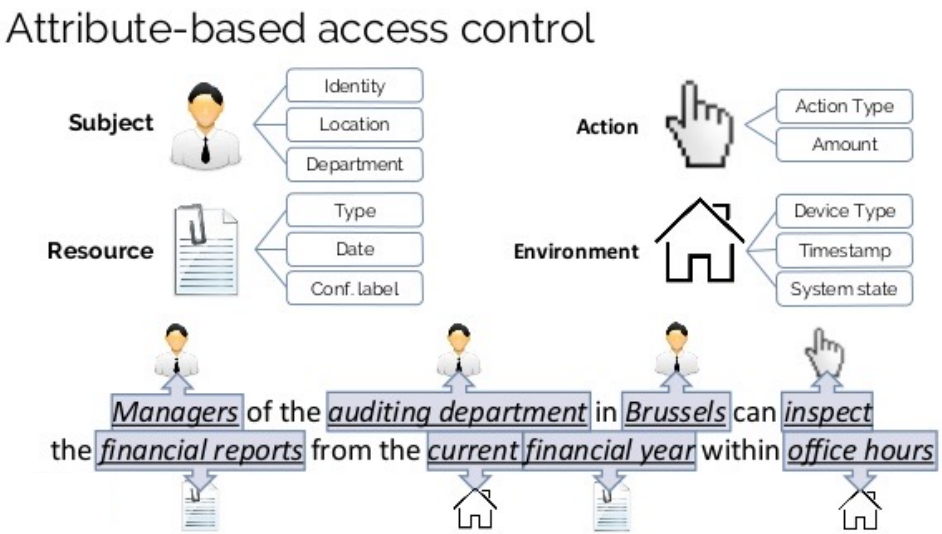
- ACL provide a simple solution to access control, but they present several drawbacks, especially when a large number of users and permissions are needed to be managed.

::.. Access Control (2/5)



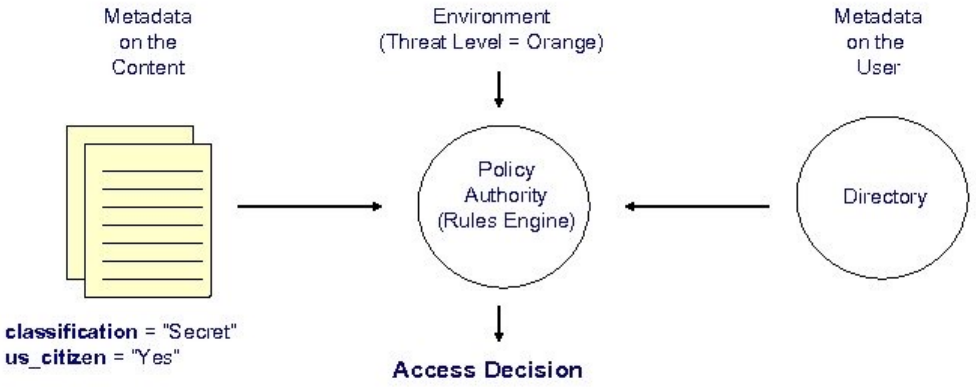
- A more advanced method makes the access to a resource based on the roles that individuals play within the organization in control of the resource. Such a solution is called Role-Based Access Control (RBAC).
- This is more scalable since it is not necessary to indicate all the permissions of the individuals to access each resource, but only the ones related to a role, associating individuals to one, or even more, roles.
- Regardless of its advantages, RBAC also suffers from several limitations, such as a coarse-grained access control and an unsuitability for cross-domain accesses.

::.. Access Control (3/5)



- Attribute-Based Access Control (ABAC) makes more fine-grained access control. Grants are decided based on the attributes possessed by the requester, the context and/or the resource itself.
- The benefit of using ABAC is the absence of the need to know the requester in advance (as required by ACL): as long as the provided attributes match with the requested ones, access is permitted. ABAC can meet some issues in a large environment where disparate attributes and access control mechanisms exist among the organizational units.

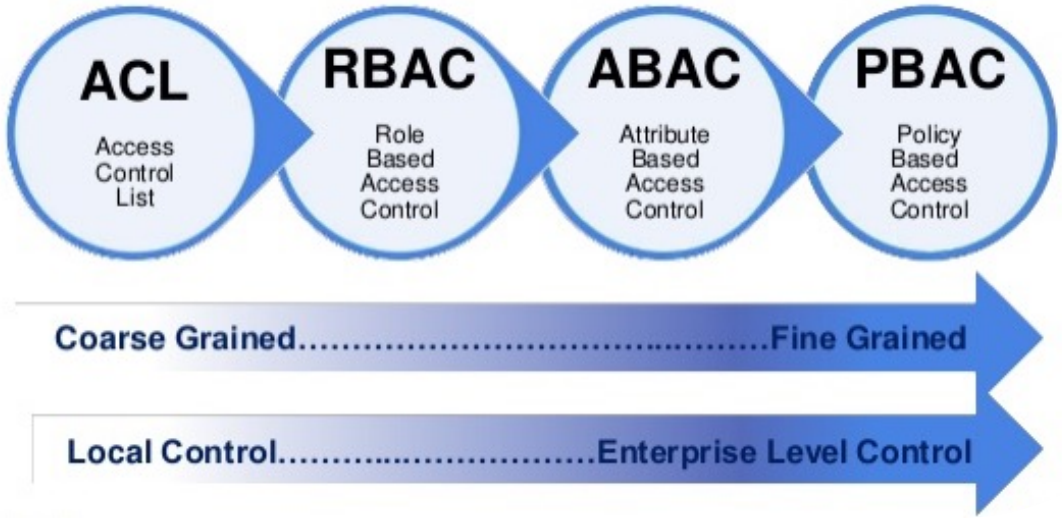
::.. Access Control (4/5)



To have a more harmonized access control across the enterprise and to achieve a more uniform model than ABAC, Policy-Based Access Control (PBAC) has been proposed.

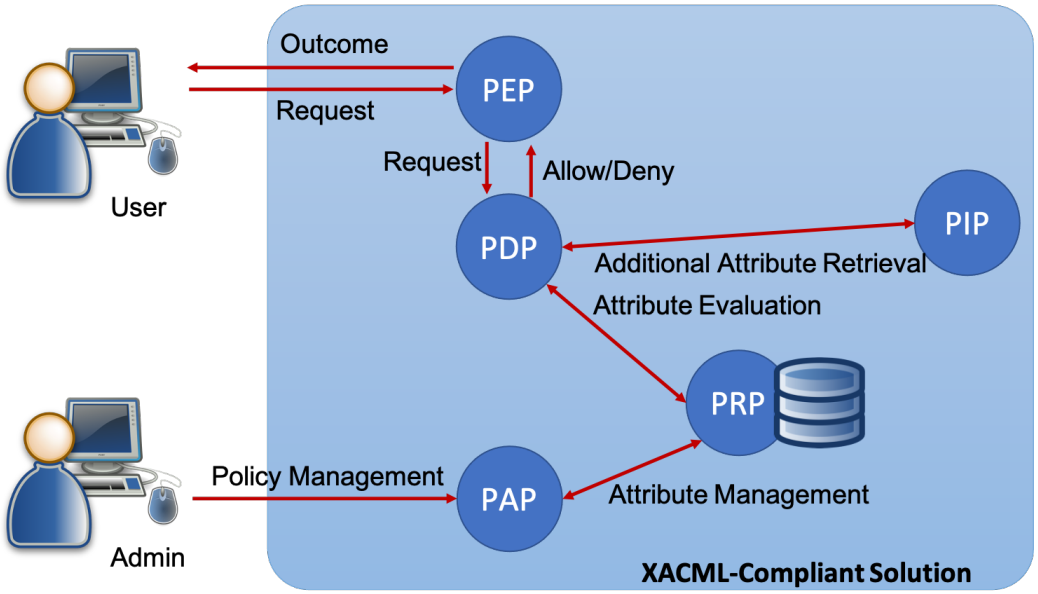
- PBAC uses digital policies comprised of logical rules to maintain and evaluate user access dynamically. PBAC is essentially a framework to evaluate a user's access based on what is known about that user at any given point in time and it focuses on the authorization component in Access Management. This model follows the zero-trust approach that is the "trust no one" security principle that defines and enforces strict access controls within an organization.

::.. Access Control (5/5)



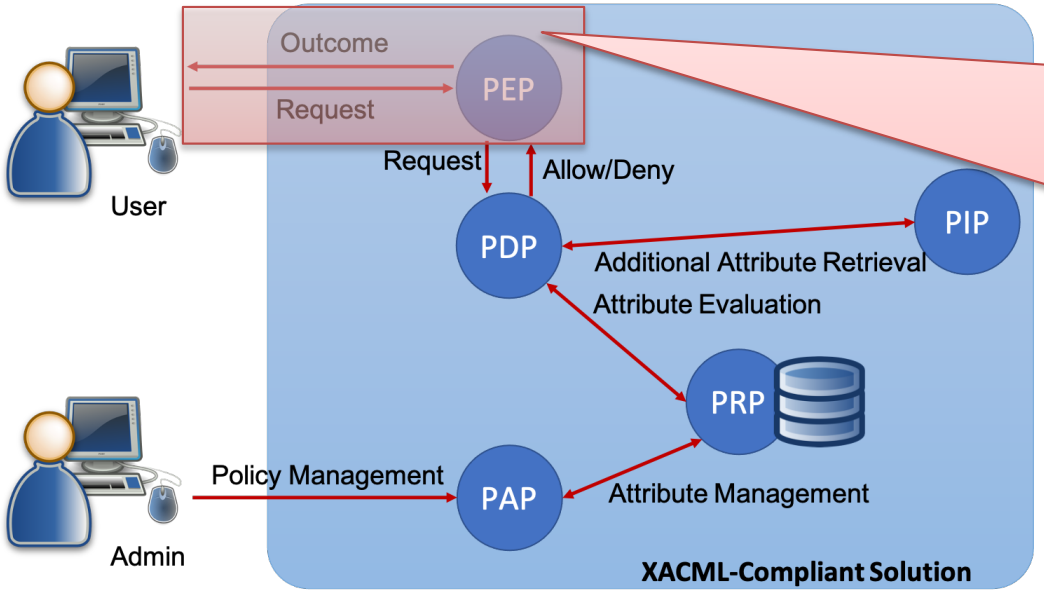
::.. XACML (1/2)

The most known implementation strategy for designing and implementing an access control service is the eXtensible Access Control Markup Language (XACML). This is an OASIS standard specifying the language to express access control policies and the architecture of a solution to evaluate them as a set of web services. The architecture in assessing access control policies is made of a set of logical components interacting with each other.



::.. XACML (1/2)

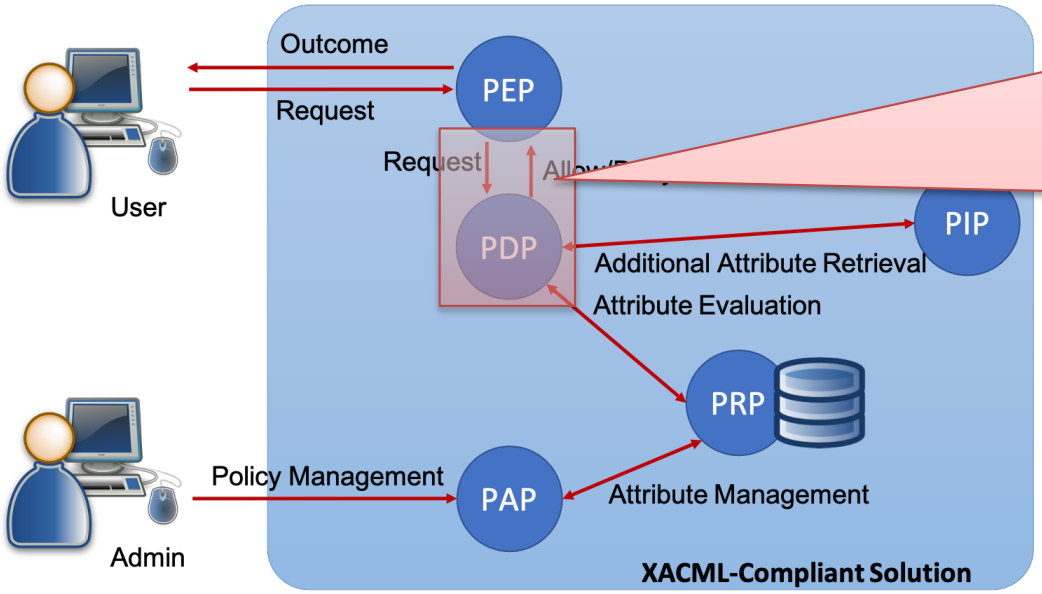
The most known implementation strategy for designing and implementing an access control service is the eXtensible Access Control Markup Language (XACML). This is an OASIS standard specifying the language to express access control policies and the architecture of a solution to evaluate them as a set of web services. The architecture in assessing access control policies is made of a set of logical components interacting with each other.



First, the Policy Enforcement Point (PEP) represents the front end protecting the resources from external requests, extracting the details for the access control verification.

::.. XACML (1/2)

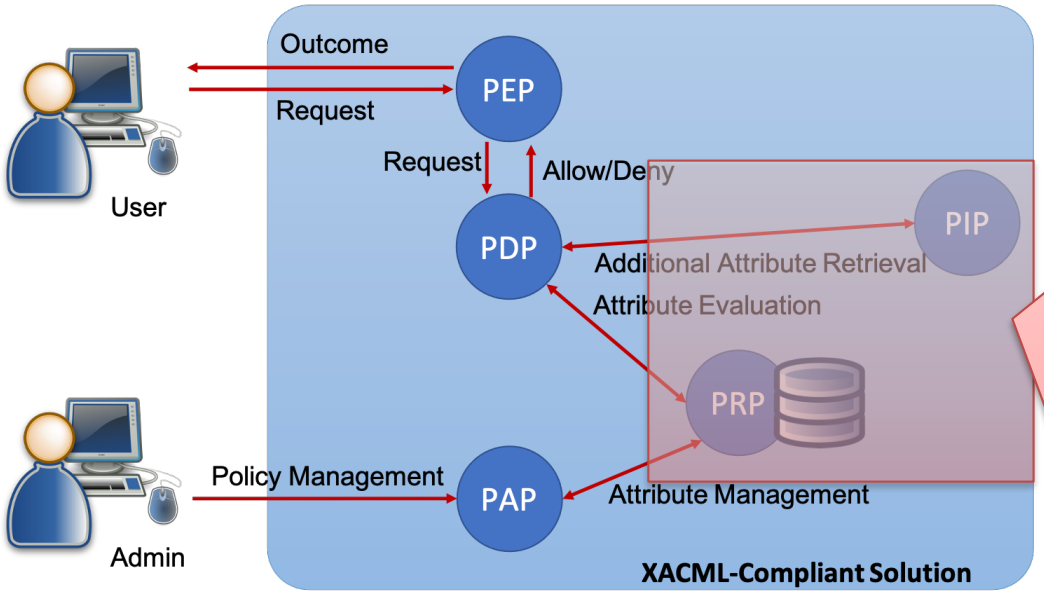
The most known implementation strategy for designing and implementing an access control service is the eXtensible Access Control Markup Language (XACML). This is an OASIS standard specifying the language to express access control policies and the architecture of a solution to evaluate them as a set of web services. The architecture in assessing access control policies is made of a set of logical components interacting with each other.



The PEP interacts with the Policy Decision Point (PDP) by passing the details extracted from the request and obtaining the decision to grate the access or define it.

::.. XACML (1/2)

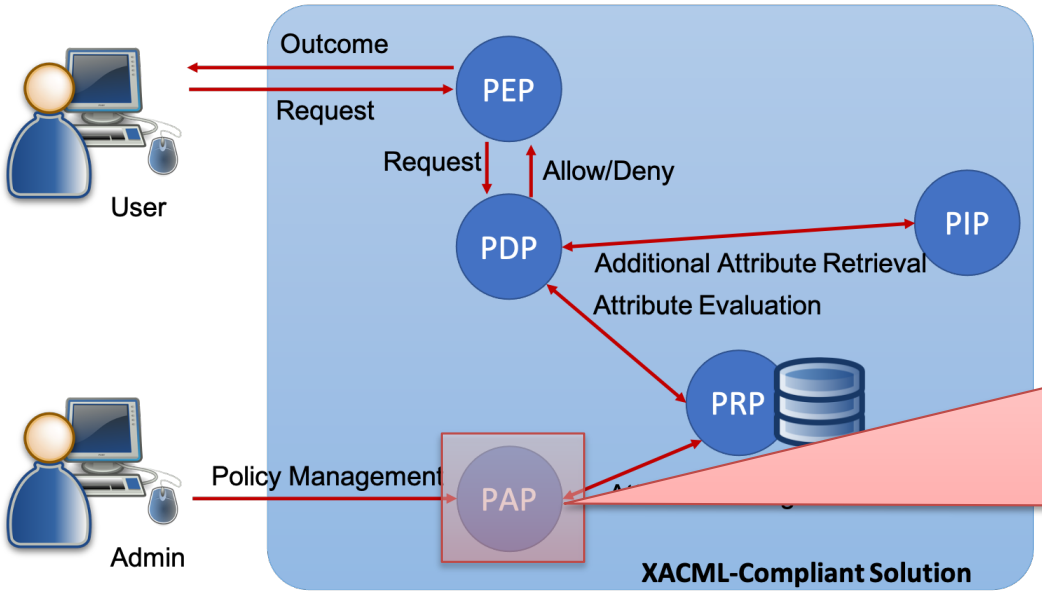
The most known implementation strategy for designing and implementing an access control service is the eXtensible Access Control Markup Language (XACML). This is an OASIS standard specifying the language to express access control policies and the architecture of a solution to evaluate them as a set of web services. The architecture in asses
made of a set of logical component



Such a decision is made by interacting with the Policy Information Point (PIP) acting as a source of attribute values (a resource, subject, environment) and the Policy Retrieval Point (PRP) responsible for storing and managing the XACML policies.

::.. XACML (1/2)

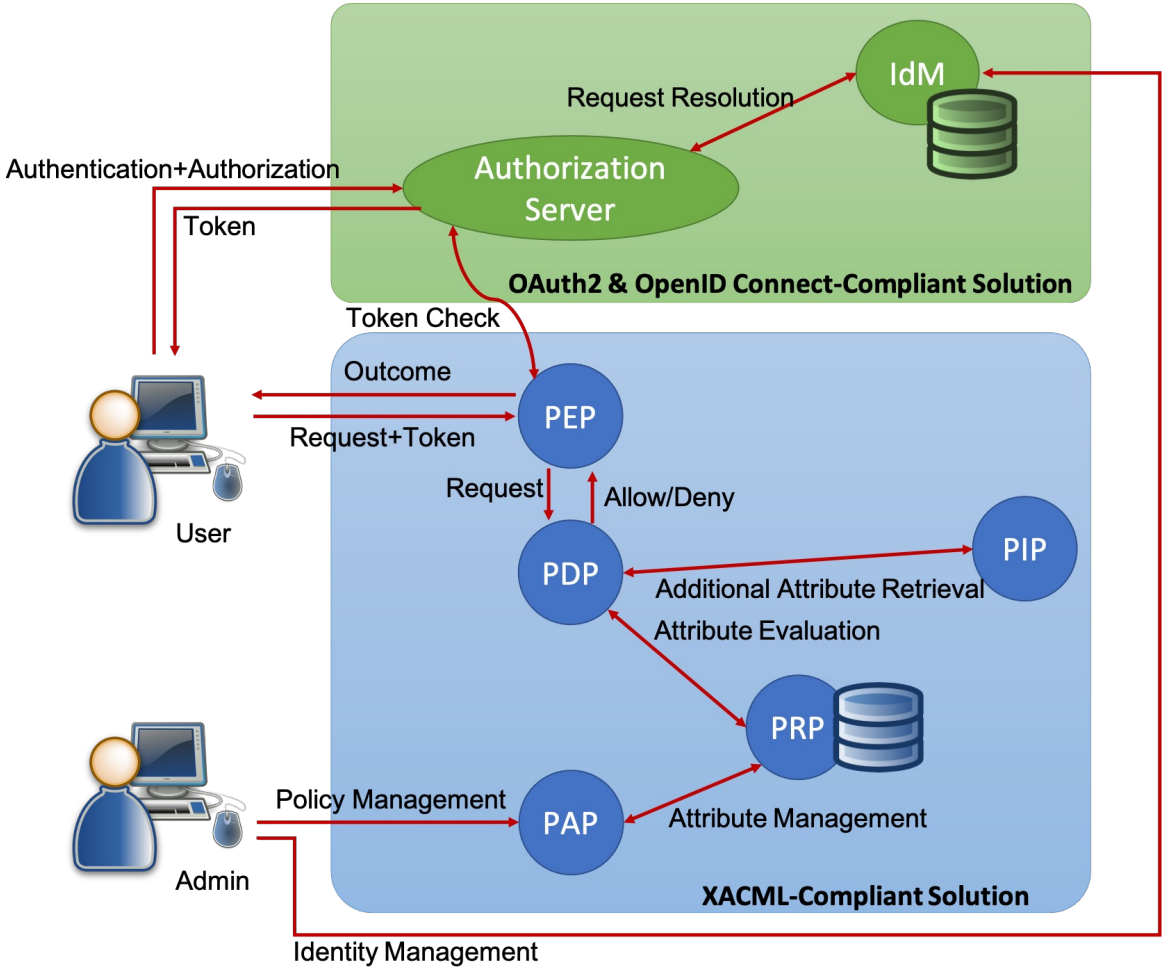
The most known implementation strategy for designing and implementing an access control service is the eXtensible Access Control Markup Language (XACML). This is an OASIS standard specifying the language to express access control policies and the architecture of a solution to evaluate them as a set of web services. The architecture in assessing access control policies is made of a set of logical components interacting with each other.



Such access control policies are administrated by the Policy Access Point (PAP) that received the administrator's requests to insert, alter, or delete XACML policies.

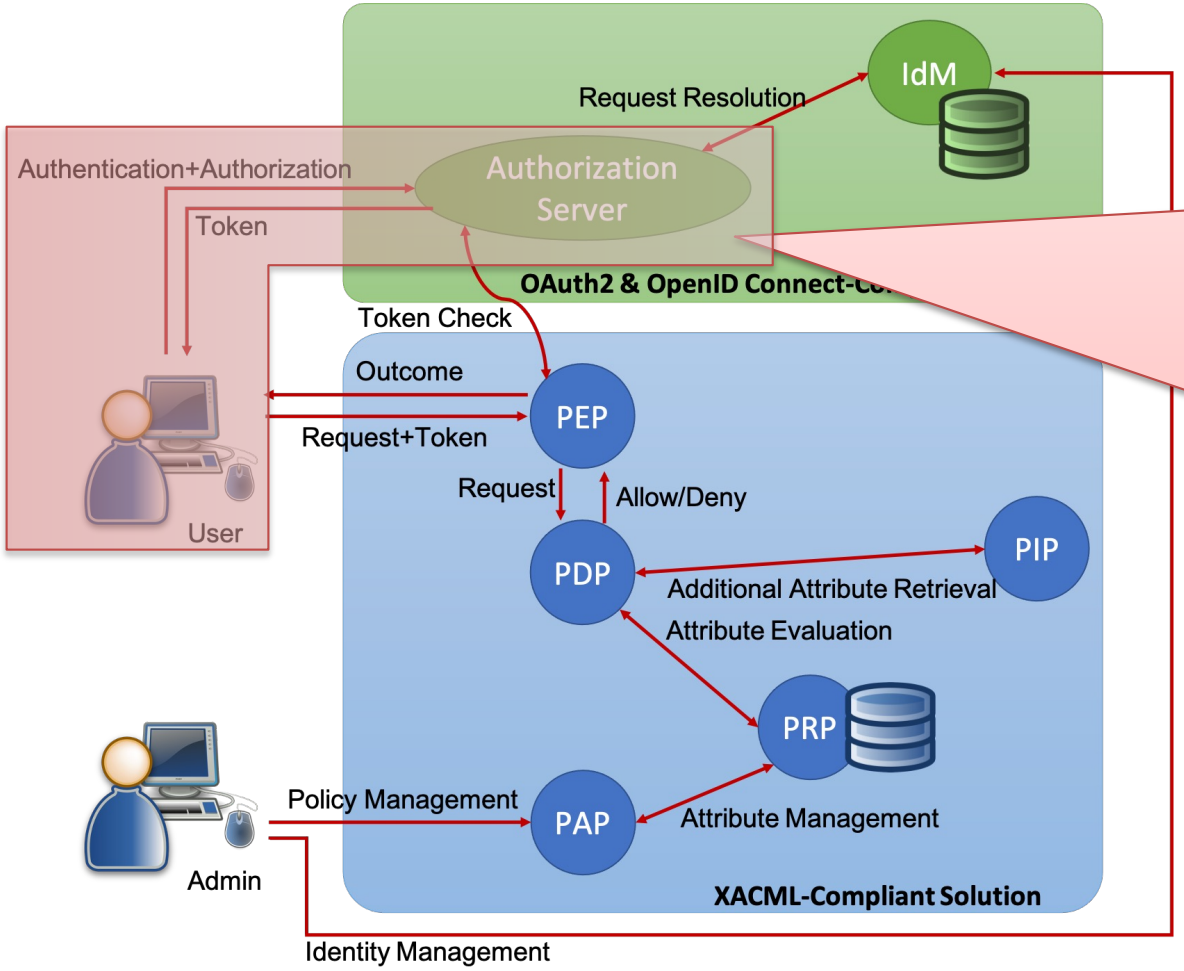
::.. XACML (2/2)

In combination with XACML, we have OAuth2, which specifies the message flows for authentication and authorization.



::.. XACML (2/2)

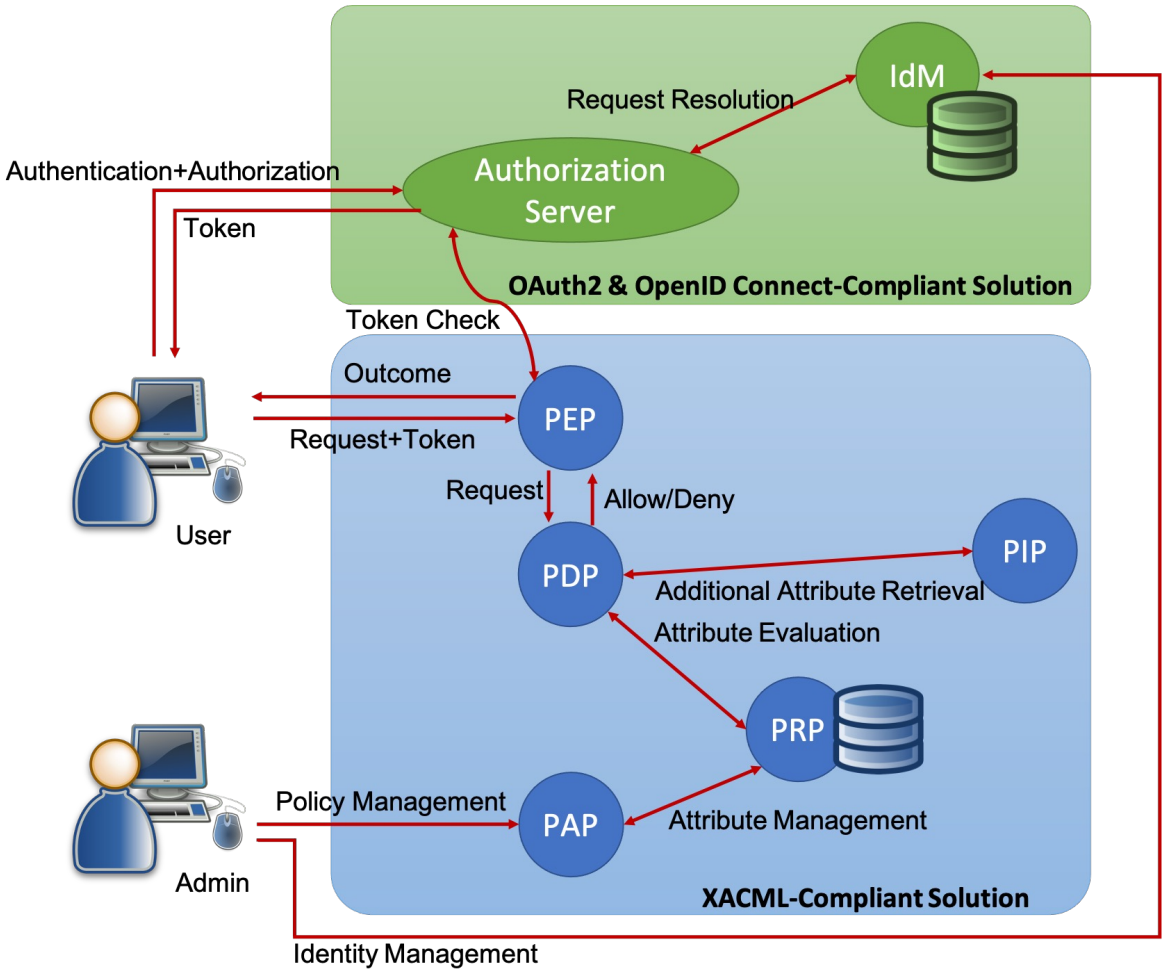
In combination with XACML, we have OAuth2, which specifies the message flows for authentication and authorization.



In the first phase, the user interacts with an authorization server, acting in accordance with the resource owner, authorized to use a particular resource, and receives an authorization token in case of a positive decision.

::.. XACML (2/2)

In combination with XACML, we have OAuth2, which specifies the message flows for authentication and authorization.



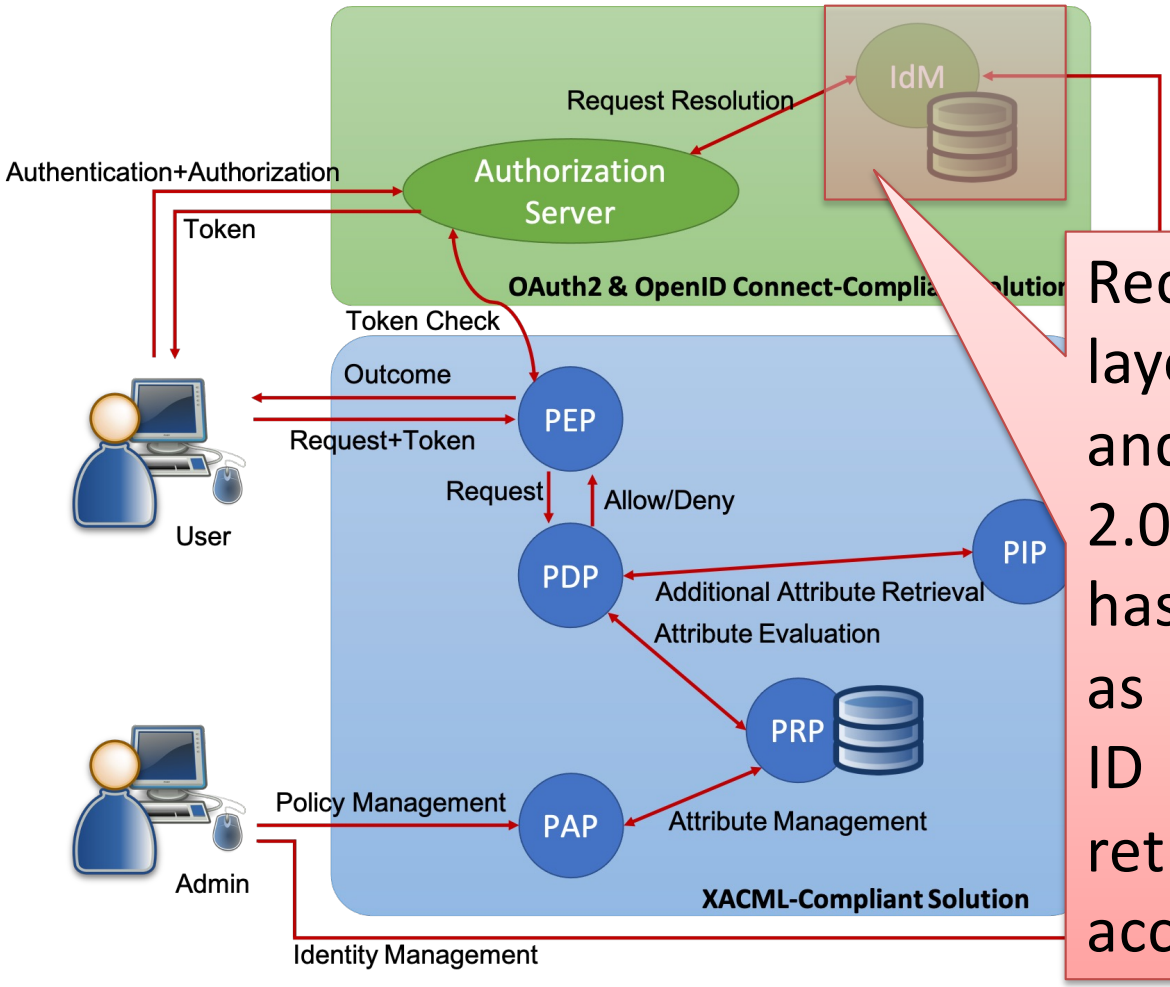
Such a protocol realizes a delegated access and pseudo-authentication and is complementary to and distinct from OpenID,.

OpenID returns an assertion of identity for the user. In contrast, with OAuth2, the user obtains a proof of permission to access the requested resource.

As obtaining an access grant may imply the user authenticating him/herself, a successful OAuth access token request is typically mistaken as an authentication method.

::.. XACML (2/2)

In combination with XACML, we have OAuth2, which specifies the message flows for authentication and authorization.



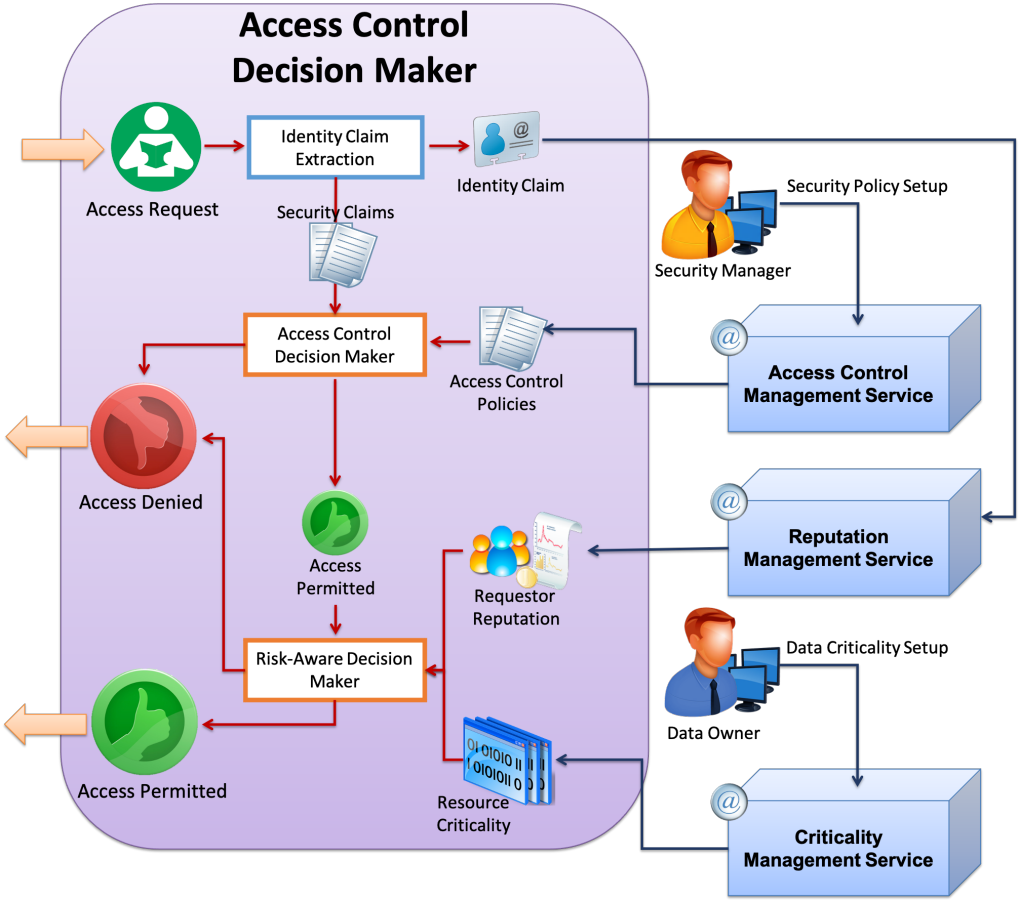
Such a protocol realizes a delegated access and pseudo-authentication and is complementary to and distinct from OpenID,.

Recently, an authentication layer compliant with OpenID and built on top of the OAuth 2.0 authorization framework has been proposed and named as OpenID Connect, where an ID token with identity claims is returned in addition to the access token.

Trust Management

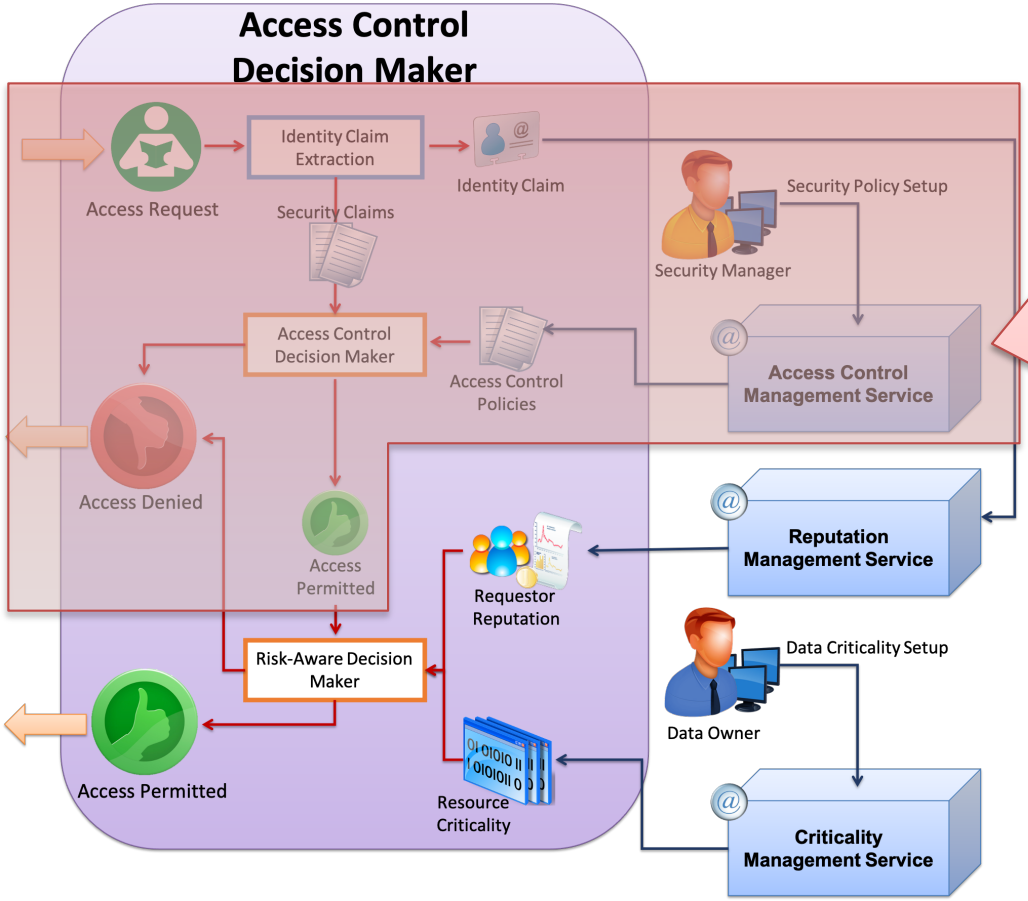
::.. Dynamic Access Control

It is important to go beyond the conventional static access control by introducing a more dynamic process to decide when granting or denying an incoming user request.



::.. Dynamic Access Control

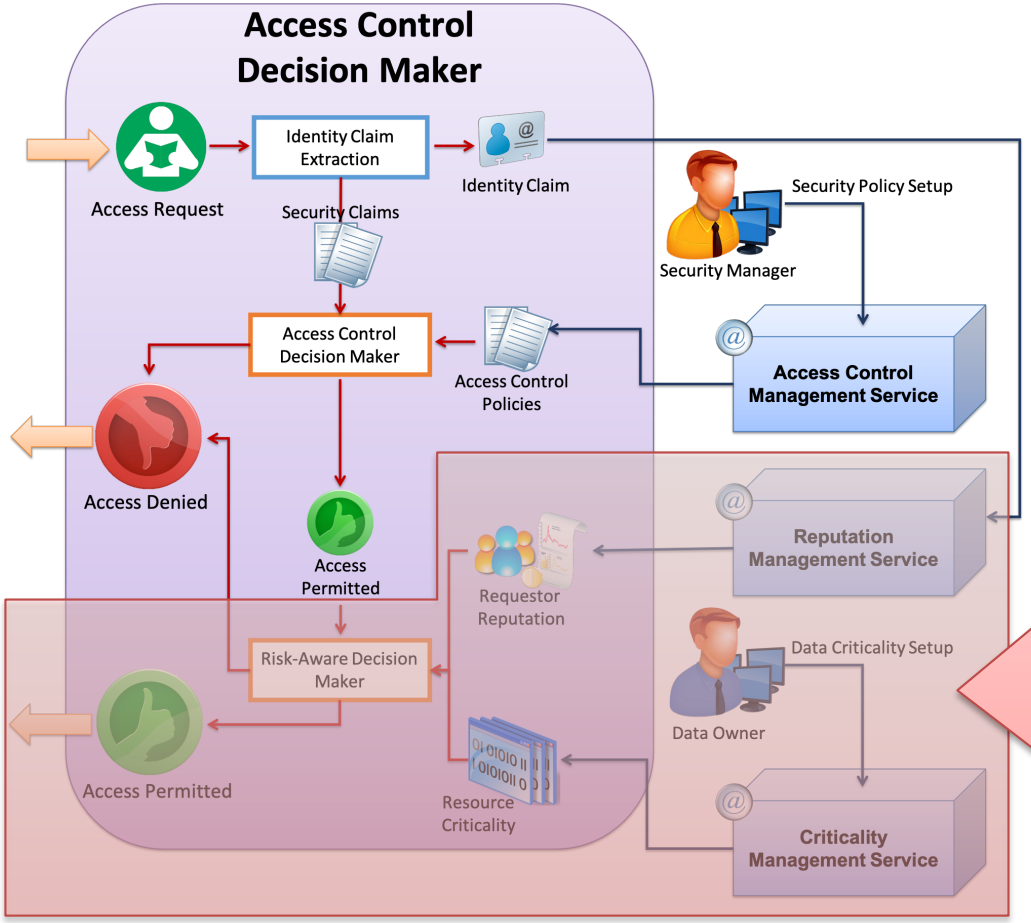
It is important to go beyond the conventional static access control by introducing a more dynamic process to decide when granting or denying an incoming user request.



The first one is a typical static approach, which takes access control decisions based on the claims exhibited by requestors and a proper set of policies defined by a security manager.

::.. Dynamic Access Control

It is important to go beyond the conventional static access control by introducing a more dynamic process to decide when granting or denying an incoming user request.



While, the second phase enhances the first one by considering the criticality of the requested data and/or operation, and the trust degree assigned to the requestor, estimated based on past interactions and collected reputation scores.

::.. Trust Management (1/3)

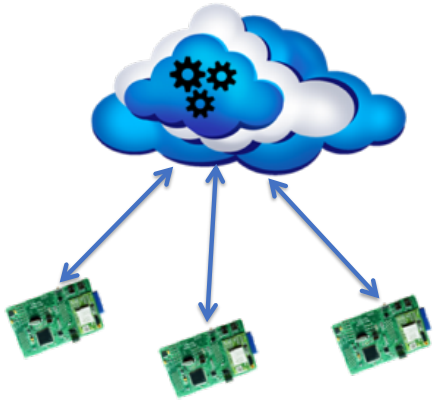
Trust management consists in having the nodes to assess the trustworthiness and correct behavior of the other nodes with which they are interacting, so as to implement a dynamic access control and being able to detect, and consequently oust, the malicious nodes despite exhibiting valid security claims.

Trust management within the IoT is far from being a completely resolved challenge, exhibiting two key issues:

- Avoiding malicious trust estimations and coping with the attacks tailored towards the trust management are essential.
- The trust management does not have to excessively drain energy from the sensors.

::.. Trust Management (2/3)

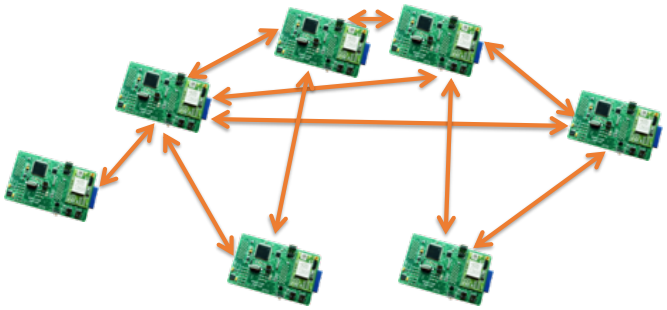
A. Central trust service



A. Simple to implement
B. Energy efficient
C. Consistent trust retrieval

A. No central management
B. Vulnerable to attacks & failures

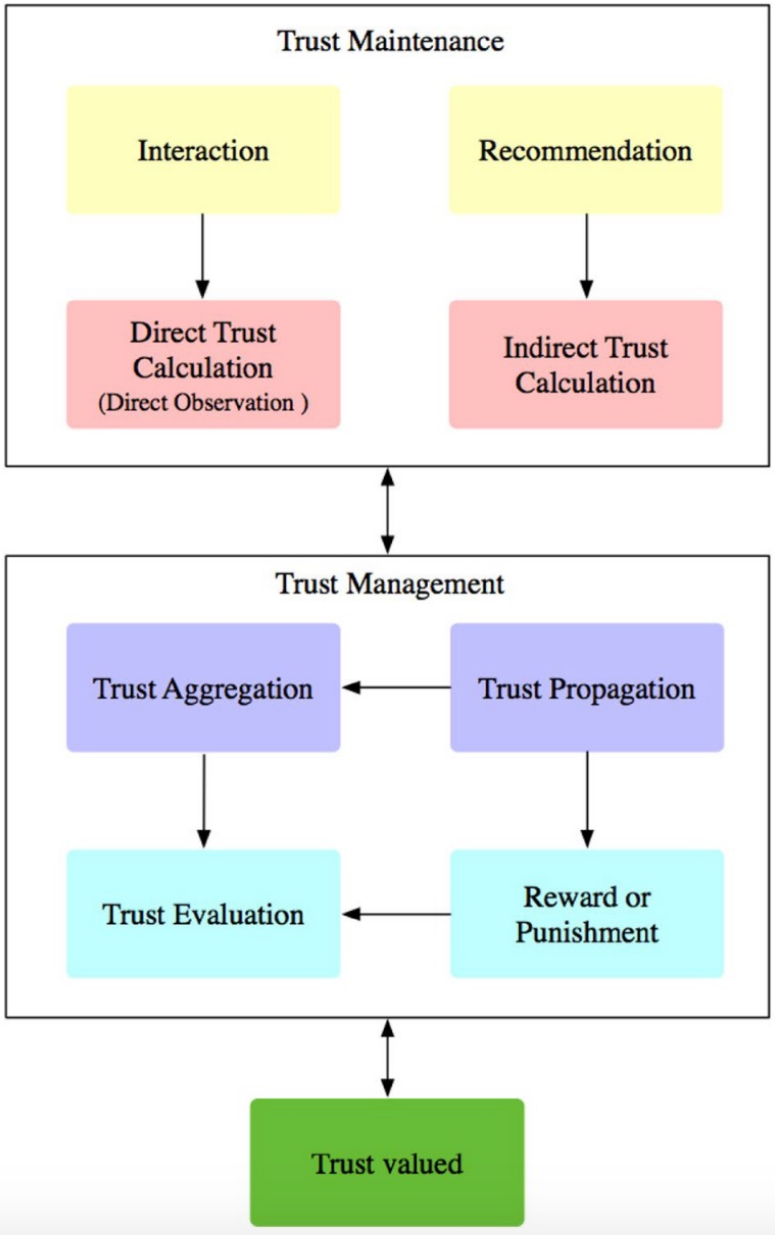
B. Distributed sensor-based trust estimation



a) Suitable for multi-tenant IoT
b) Robust to failures

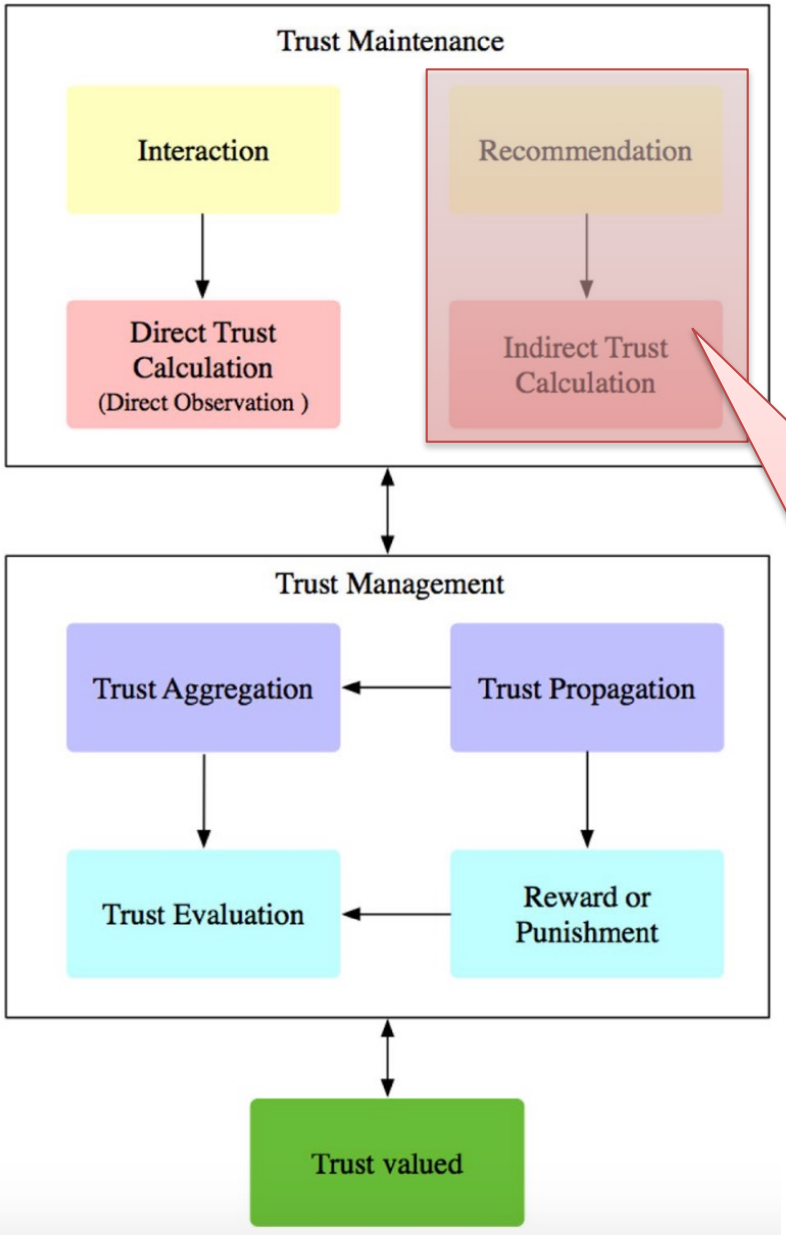
a) Complex to implement
b) Energy inefficient
c) Vulnerable to attacks and inconsistencies

::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

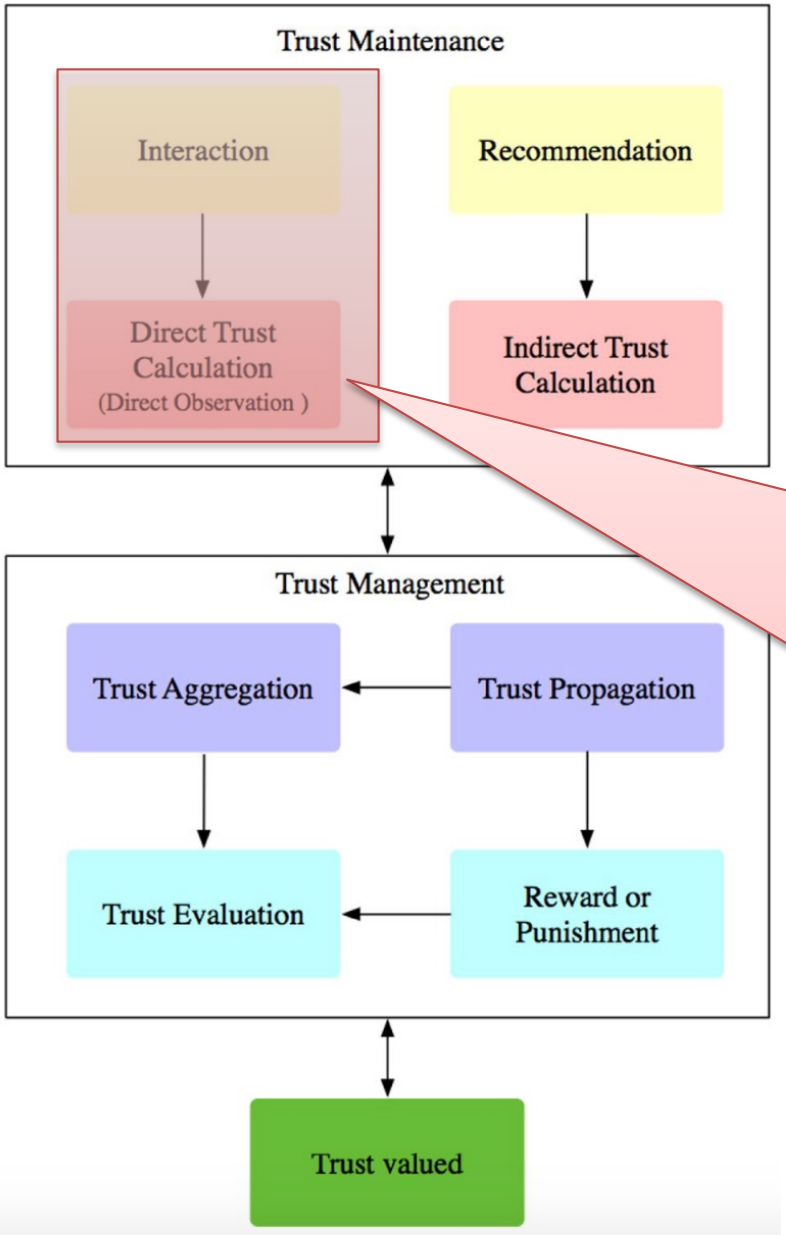
::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

When an evaluating node is incapable of directly assessing an encountered element's behavior, it builds a reliable trust path based on the indirect knowledge and opinions obtained from an intermediate node or a chain of trusted parties.

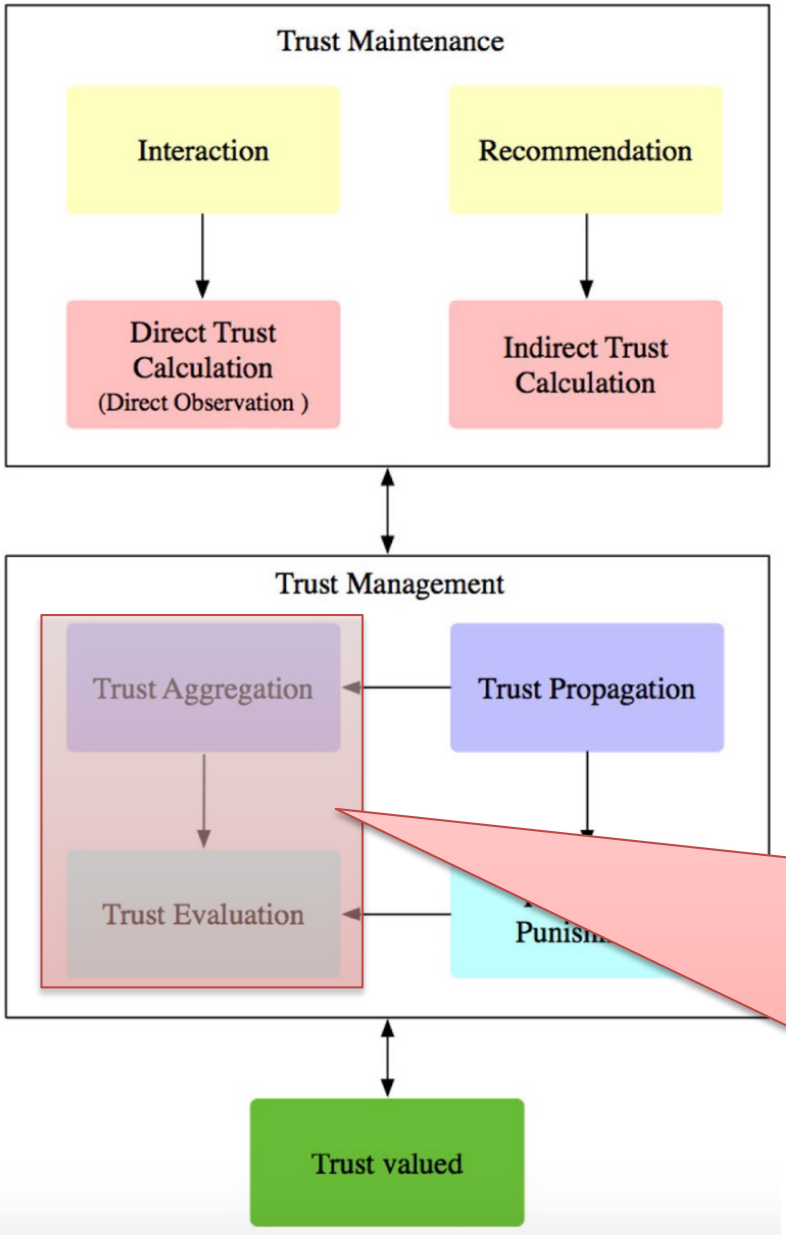
::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

A node infers first-hand trust information by its personal experience which gathers either through one-to-one interaction with neighbours, or direct observation of nodes' social behaviors or attitudes towards one another.

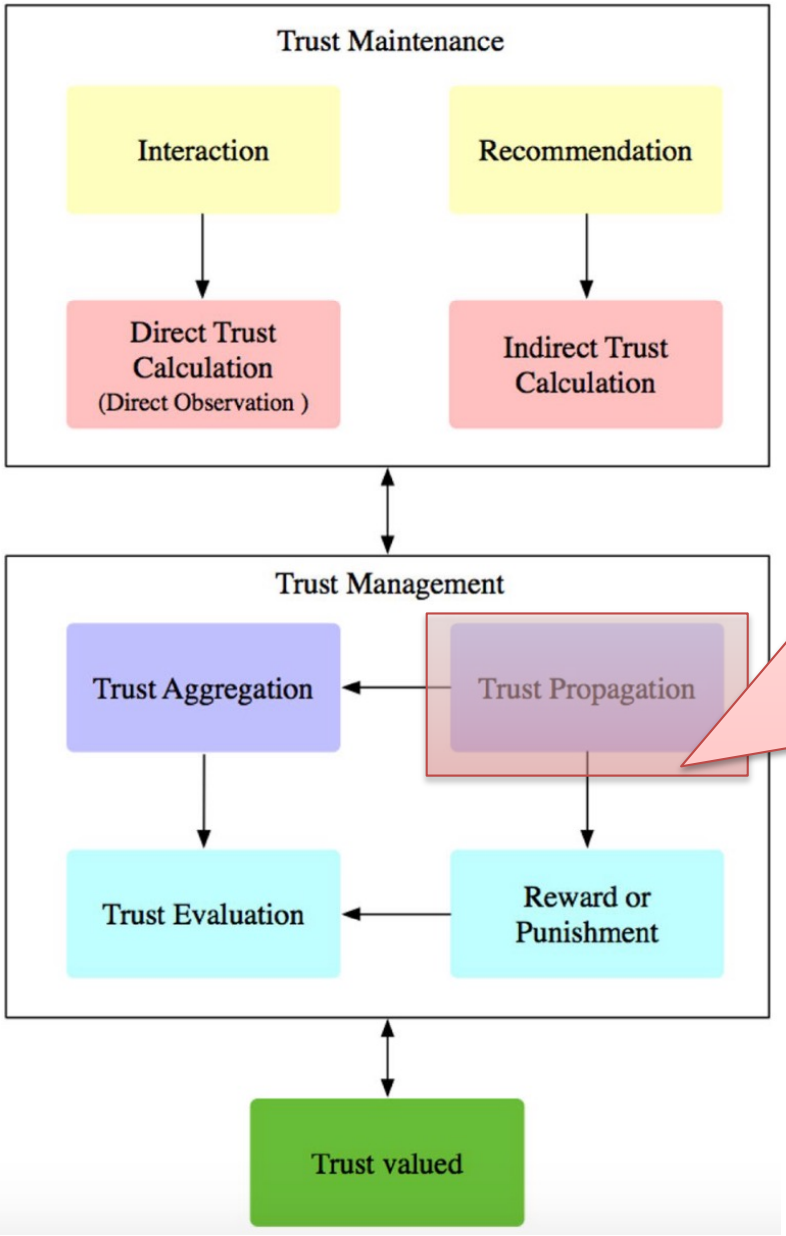
::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

To achieve overall trustworthiness degree, a node aggregates per-sonal direct trust with received multiple recommendations. In this respect, trust aggre-gation method detects and excludes slandering recommendation by assigning a low trust weight to malicious nodes.

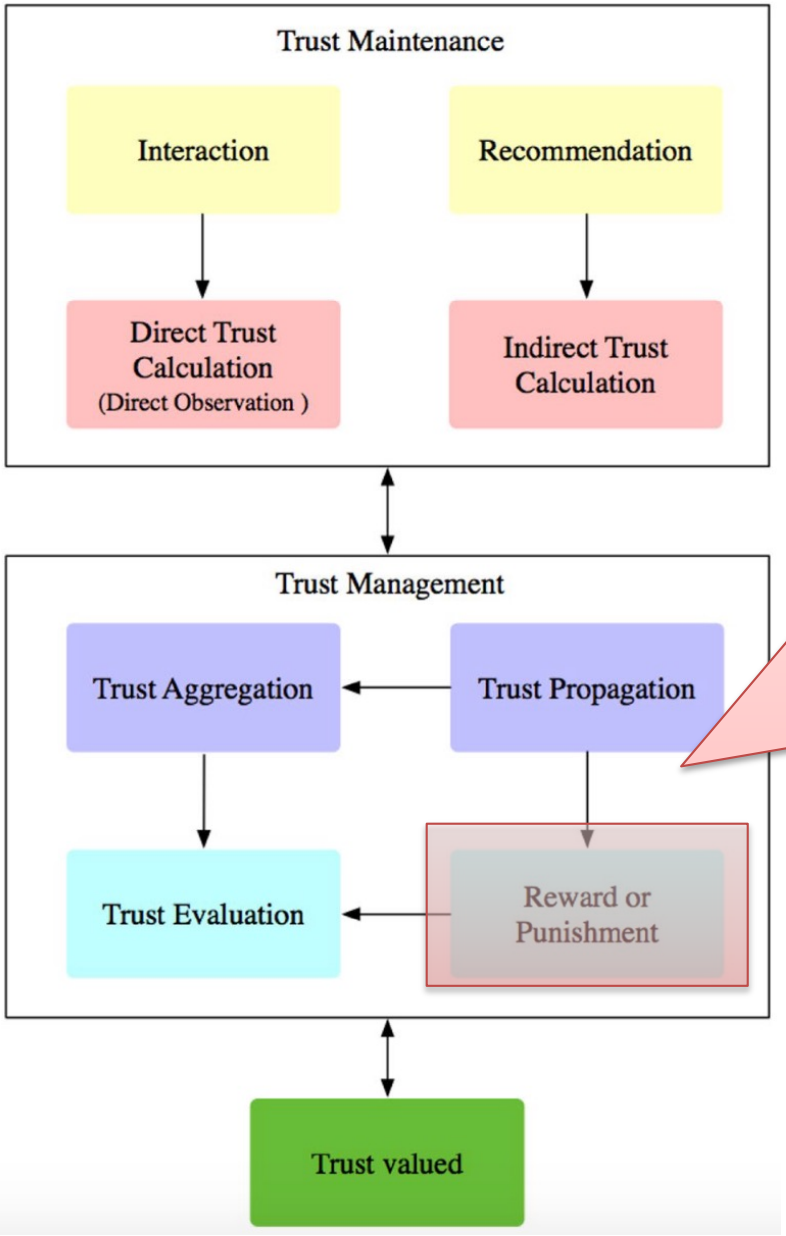
::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

After collecting the trust factor from a target node and evaluating trust value by the proposed model, the final result is propagated as recommendations. As soon as a node receives a recom-menddation, it should run the aggregating process.

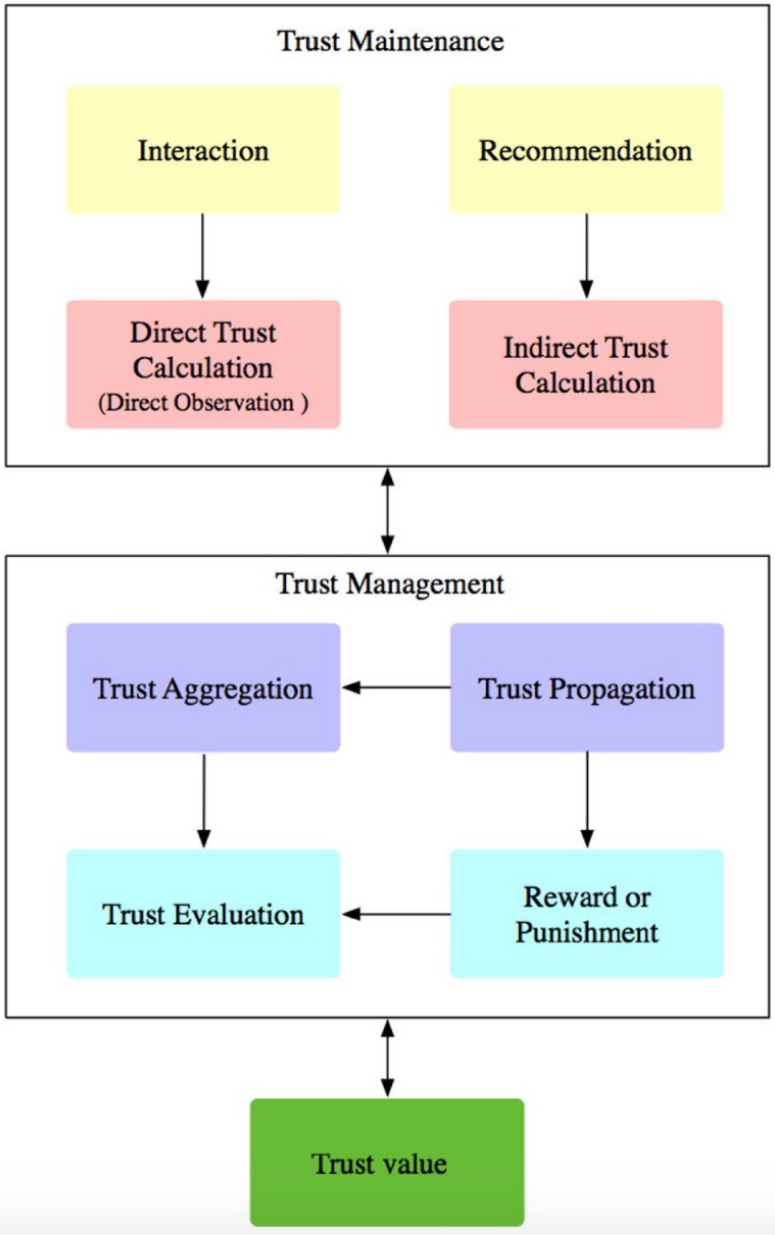
::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

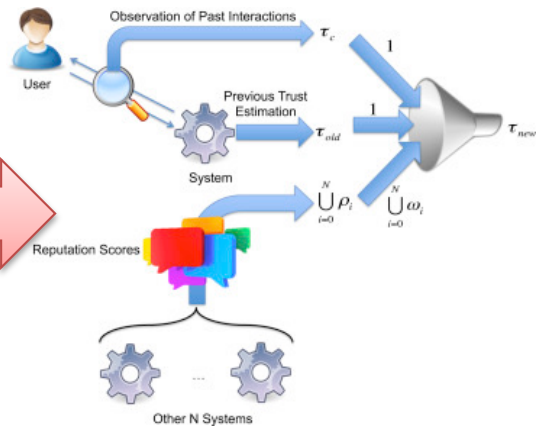
As soon as completion of the transaction, the requested either punishes or rewards the node's behavior either by positive or negative feedback. Nodes with high trust-worthiness are involved in the next interaction and low score nodes are certainly isolated.

::.. Trust Management (3/3)



A trust-based recommendation model consists of three fundamental modules: trust maintenance, trust management, trust value.

Trust Composition	QoS + Social
Trust Propagation	Distributed
Trust Aggregation	Static weighted sum
Trust Update	Event-driven + Time-driven
Trust Formation	Multi-trust



Auditing

::.. Audit (1/5)

Auditing consists of collecting, storing, and distributing all the information related to the received requests and consequent outcomes (jointly with the respective identity of the user that has requested the operation).

Auditing represents a pivotal element to achieve a high degree of security by allowing the detection of attempted security violations aimed at breaking the mechanisms used to protect the overall system and promotes an improvement of the security mechanisms to avoid future successful violations.

Several regulations for security in different application domains impose the adoption of auditing within the systems so as to enforce the achievable security guarantees.

::.. Audit (2/5)

- The first thing to establish is the audit subject. ISACA's IS Audit and Assurance Standards* has defined IoT as anyone or anything carrying embedded software that enables interaction with other animate or inanimate objects across networks. Interaction entails sharing and processing information to influence decision-making and/or actions with or without human intervention.

  The key is to consider all IoT devices in use at your enterprise and to determine the audit subject(s). You need to answer the key question: What are you auditing?
- Once we have decided what we are auditing, we need to establish the objective of the audit. Why are we auditing it?

*https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/standards-guidelines-tools-and-techniques

::.. Audit (3/5)

From an auditor's perspective, it is advisable to adopt a risk-based view and define the objectives accordingly.

Risk Category	Examples
Business	• Health and safety • Regulatory compliance • User privacy • Unexpected costs
Operational	• Inappropriate access to functionality • Shadow usage • Performance
Technical	• Device vulnerabilities • Device updates • Device management

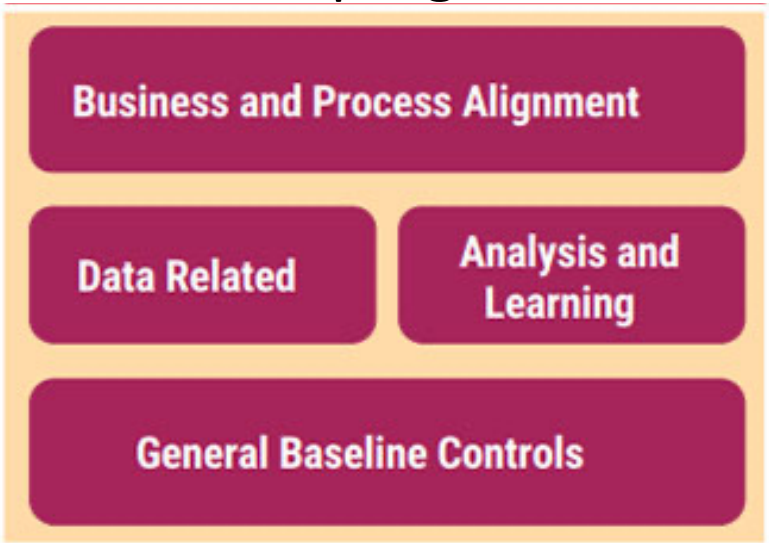
Source: Adapted from ISACA, *Internet of Things: Risk and Value Consideration*, USA, 2015. Reprinted with permission.

- What are the limits to the audit? As the devices are not just the sensors but include supporting infrastructure such as the connectivity equipment, the cloud or other storage means, and the algorithms used for processing the data.

::.. Audit (4/5)

Conducting a risk assessment is critical in setting the final scope of a risk-based audit.

- At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program. There are no universally accepted standards for quality, safety or durability. Similarly, there are no universally accepted audit/assurance programs.

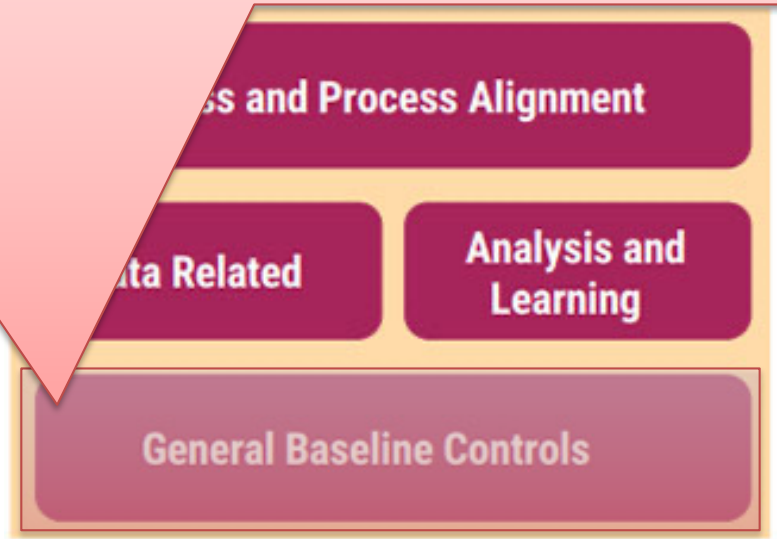


::.. Audit (4/5)

Conducting a risk assessment is critical in setting the final scope of a risk-based audit.

- At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit

General baseline controls—Minimum controls that need to be applied to all aspects of the technology.



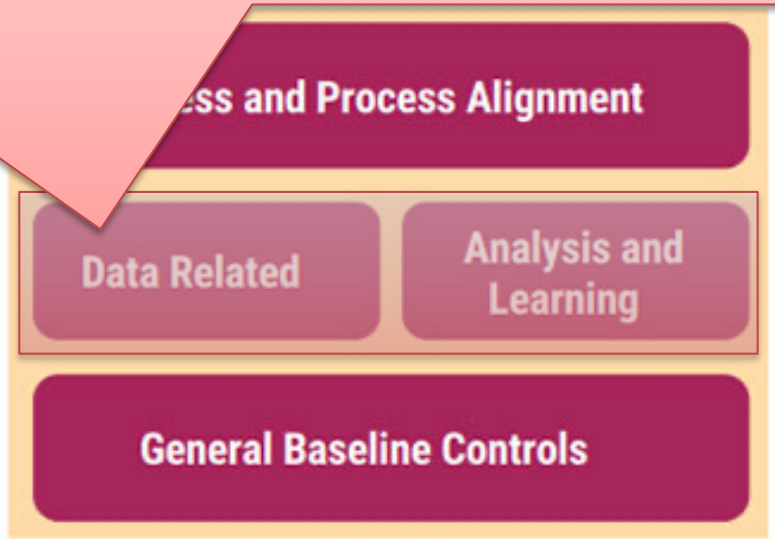
::.. Audit (4/5)

Conducting a risk assessment is critical in setting the final scope of a risk-based audit.

- At this stage of the audit process, the audit team should

Data-related controls—Such as controls that apply to the data forming a key part of IoT.

Analysis and learning-related controls—Applied to ensure that the analysis is ethical and enables trusted use of the data and that outcomes of analysis can be applied to business decision-making.



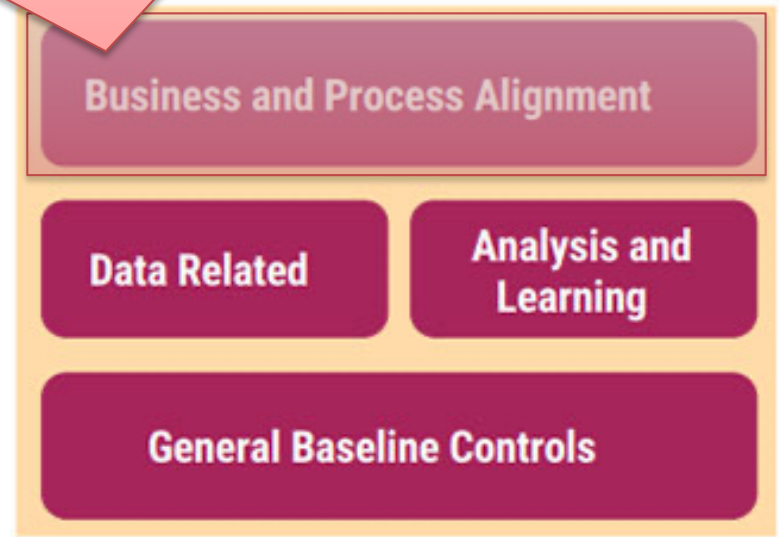
::.. Audit (4/5)

Conducting a risk assessment is critical in setting the final scope of a risk-based audit.

- At this stage of the audit process, the audit team should

Business and process alignment—Related aspects which ensure that the IoT implementation is aligned to business needs and that business benefits are delivered as required.

universally a audit/assurance programs.



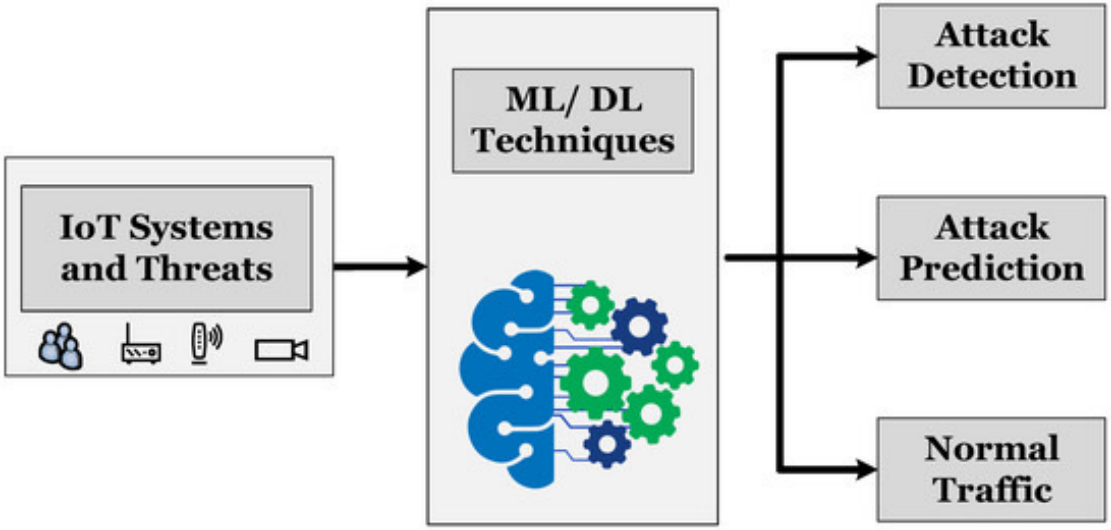
::.. Audit (5/5)

Applicable sources of assurance for each of the previously mentioned components are the following ones. Some of these relate directly to the IoT while others are more generic and should be applied to relevant IoT components.

Area	Source of Assurance
General baseline controls	• Open Web Application Security Project (OWASP) IoT Security Guidance[16] • Global System for Mobile Communications Association (GSMA) IoT Security Assessment[17] • Future Proofing the Connected World[18] • US Department of Defense Security Technical Implementation Guide (STIG)[19] • CIS Benchmarks[20]
Data related	• OWASP IoT Security Guidance[21] • GSMA IoT Security Assessment • Future Proofing the Connected World[22] • *COBIT® 5: Enabling Information*[23] • US Health Insurance Portability and Accountability Act (HIPAA) Audit/Assurance Program[24] • *ISACA® Privacy Principles, Governance and Management Program Guide*[25] • *Auditing Data Privacy*[26] • General Data Protection Regulation (GDPR) Readiness, Assessment and Compliance[27]
Analysis and learning	• OWASP IoT Security Guidance[28] • GSMA IoT Security Assessment • Future Proofing the Connected World[29] • *ISACA Privacy Principles, Governance and Management Program Guide*[30] • *Auditing Data Privacy*[31] • General Data Protection Regulation (GDPR) Readiness, Assessment and Compliance[32] • Bias Testing for Generalized Machine Learning Applications[33]
Business and process alignment	• COBIT® 5[34]

::.. IDS (1/3)

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

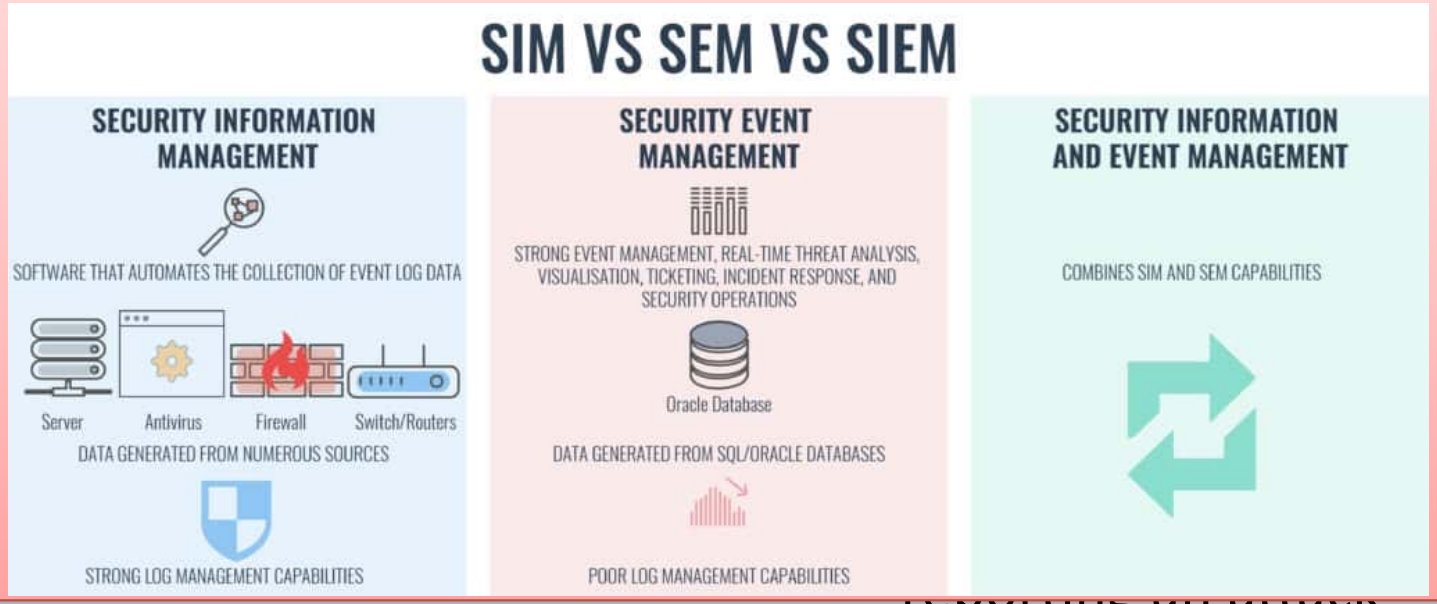


Most IDSs have a common structure that includes: (1) a data gathering module collects data, which possibly contains evidence of an attack, (2) an analysis module detects attacks after processing that data, and (3) a mechanism for reporting an attack

::.. IDS (1/3)

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs fro[illegible]urces and uses alarm filtering techniques to

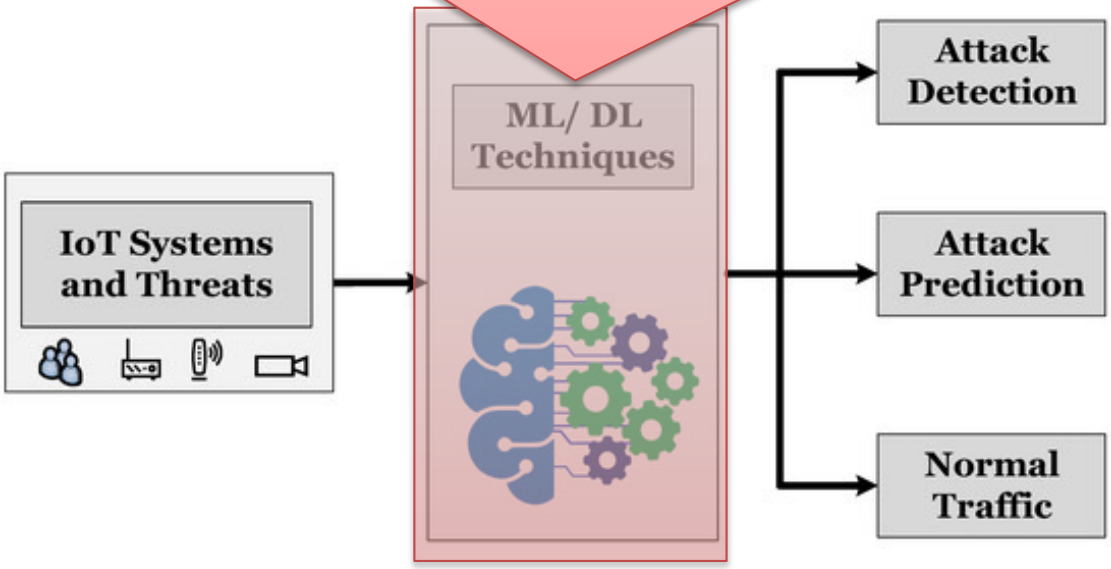
SIEM products provide real-time analysis of security alerts generated by network hardware and applications.



reporting an attack

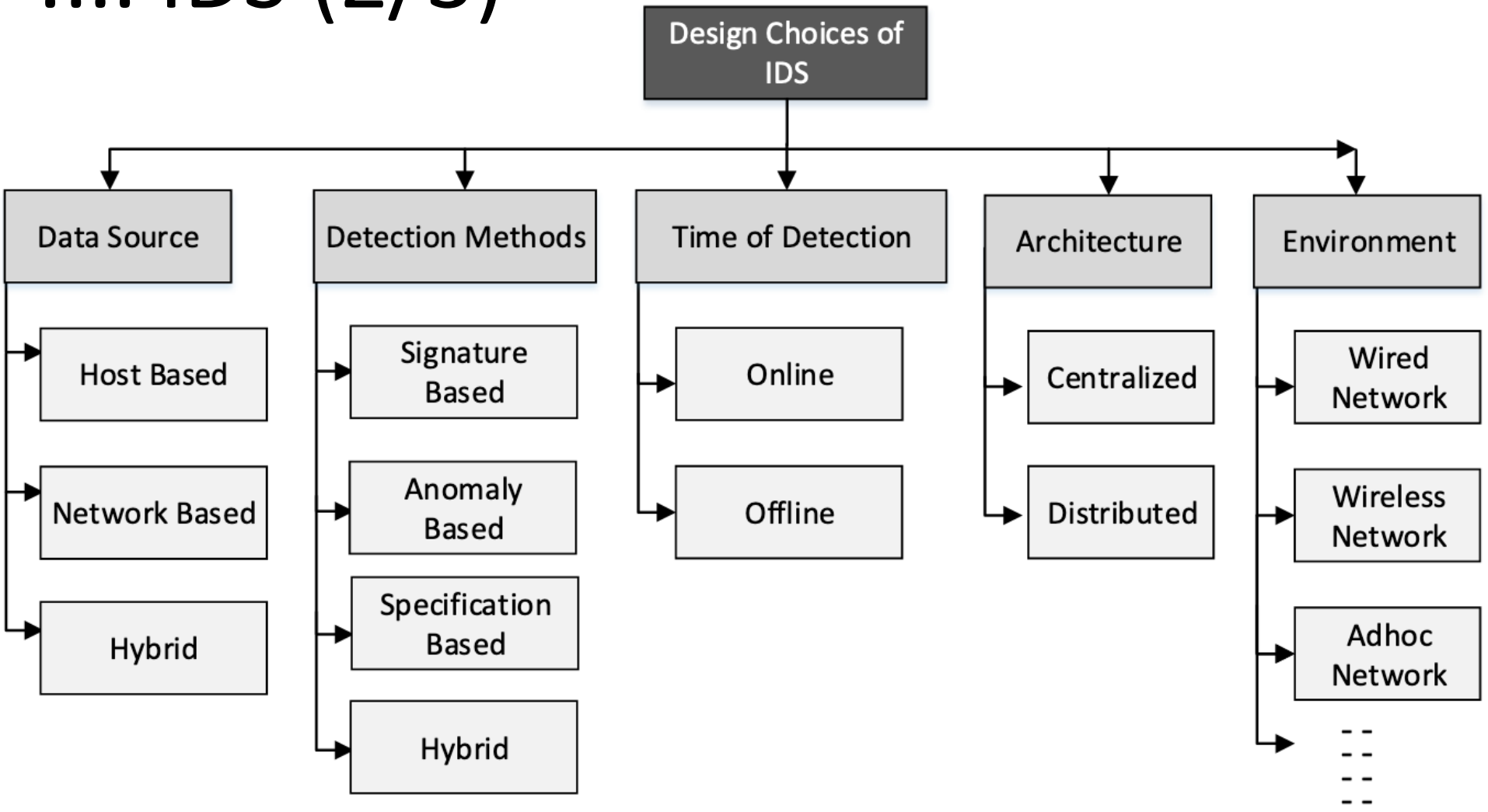
::.. IDS (1/3)

The Analysis module can be implemented using various techniques and methods, however, Machine Learning (ML) and Deep Learning (DL) are more suitable to learn benign and anomalous behavior based on how IoT devices and systems interact with one another. Furthermore, ML/DL methods can predict new attacks, which are often different from previous attacks through learning from existing legitimate samples.



Most IDSs have a common structure that includes: (1) a data gathering module collects data, which possibly contains evidence of an attack, (2) an analysis module detects attacks after processing that data, and (3) a mechanism for reporting an attack

::.. IDS (2/3)



The main differences in the design choices for IDSs depends on various factors and design choices.

::.. IDS (3/3)

- Signature-based detection techniques contain a repository of attack signatures and compares the network traffic or system actions against this repository of signatures. As soon as any match is found, a detection alert is raised.
- Anomaly-based detection techniques rely on a baseline normal behavior profile for the monitored environment. This normal baseline is then used for comparison of system actions at any given moment. Any deviations out of bounds of the allowed threshold are reported without providing any classification for the type of attack detected.
- In anomaly-based techniques, normal behavior is learned, whereas for specification-based techniques it needs to be manually specified through a repository of rules and associated ranges of deviations by a human expert.