Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Application Security
Identity & Access Management

Agenda

- Introduction
- IAM Processes
- IAM Services
- LDAP
- AAA Introduction
- Authentication
  - Concepts, Methods, Factors
- Authorizations
- Accounting
- Access Control
  - Models, Solutions

Introduction

Identity and access management (IAM) is the security discipline that enables

the right individuals to access

the right resources at

the right times for

the right reasons.

Gartner

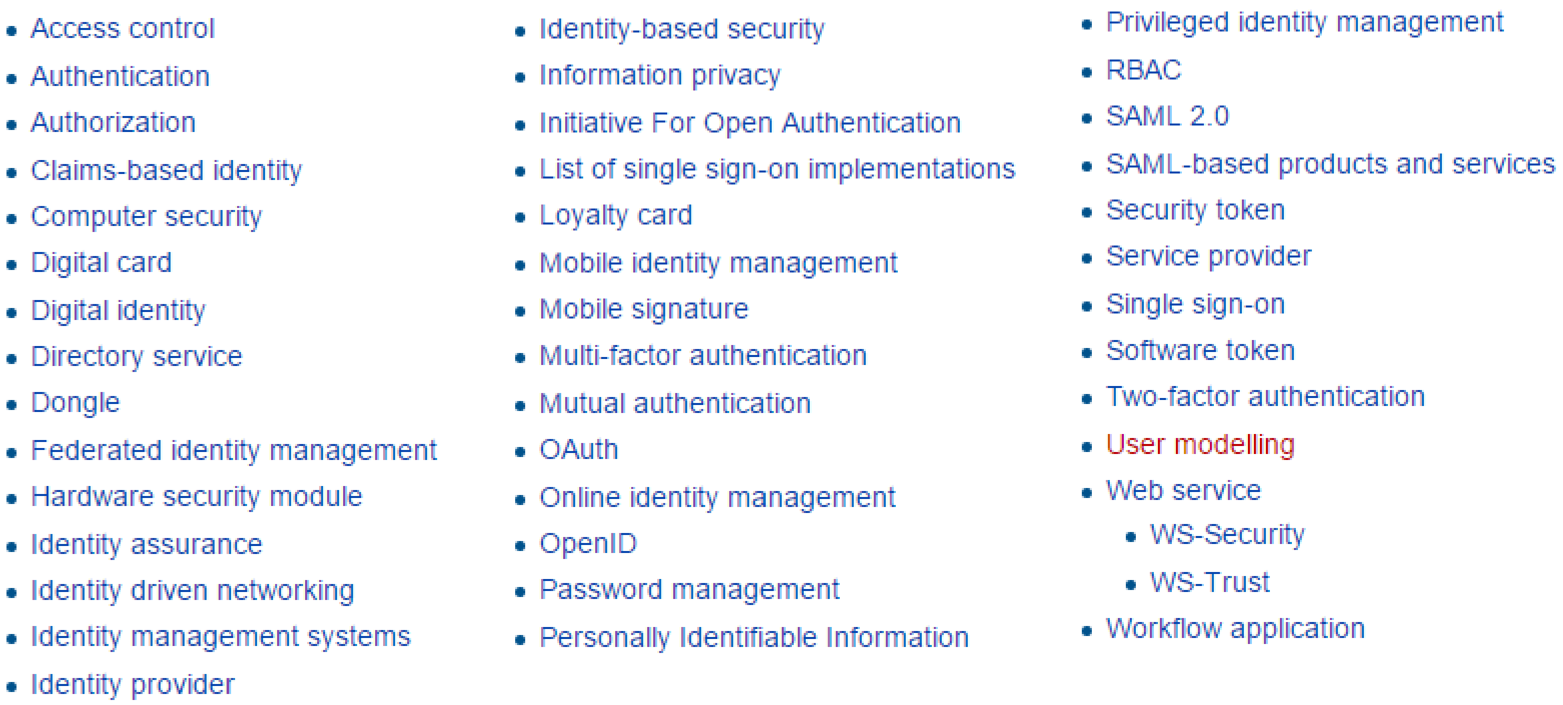
http://www.gartner.com/it-glossary/identity-and-access-management-iam

Introduction

- Authentication, Authorization, Accounting (AAA)
- Access Control
- AAA & Directory Services
- Single Sign-On (SSO)
- User Provisioning and Deactivation
- Access Management
- Delegated administration
- Password Administration and Synchronization
- Federated Identity
- Trunsitive trust/authentication

Introduction

- Related topics



- Access control
- Authentication
- Authorization
- Claims-based identity
- Computer security
- Digital card
- Digital identity
- Directory service
- Dongle
- Federated identity management
- Hardware security module
- Identity assurance
- Identity driven networking
- Identity management systems
- Identity provider
- Identity-based security
- Information privacy
- Initiative For Open Authentication
- List of single sign-on implementations
- Loyalty card
- Mobile identity management
- Mobile signature
- Multi-factor authentication
- Mutual authentication
- OAuth
- Online identity management
- OpenID
- Password management
- Personally Identifiable Information
- Privileged identity management
- RBAC
- SAML 2.0
- SAML-based products and services
- Security token
- Service provider
- Single sign-on
- Software token
- Two-factor authentication
- User modelling
- Web service
  - WS-Security
  - WS-Trust
- Workflow application

https://en.wikipedia.org/wiki/Identity_management

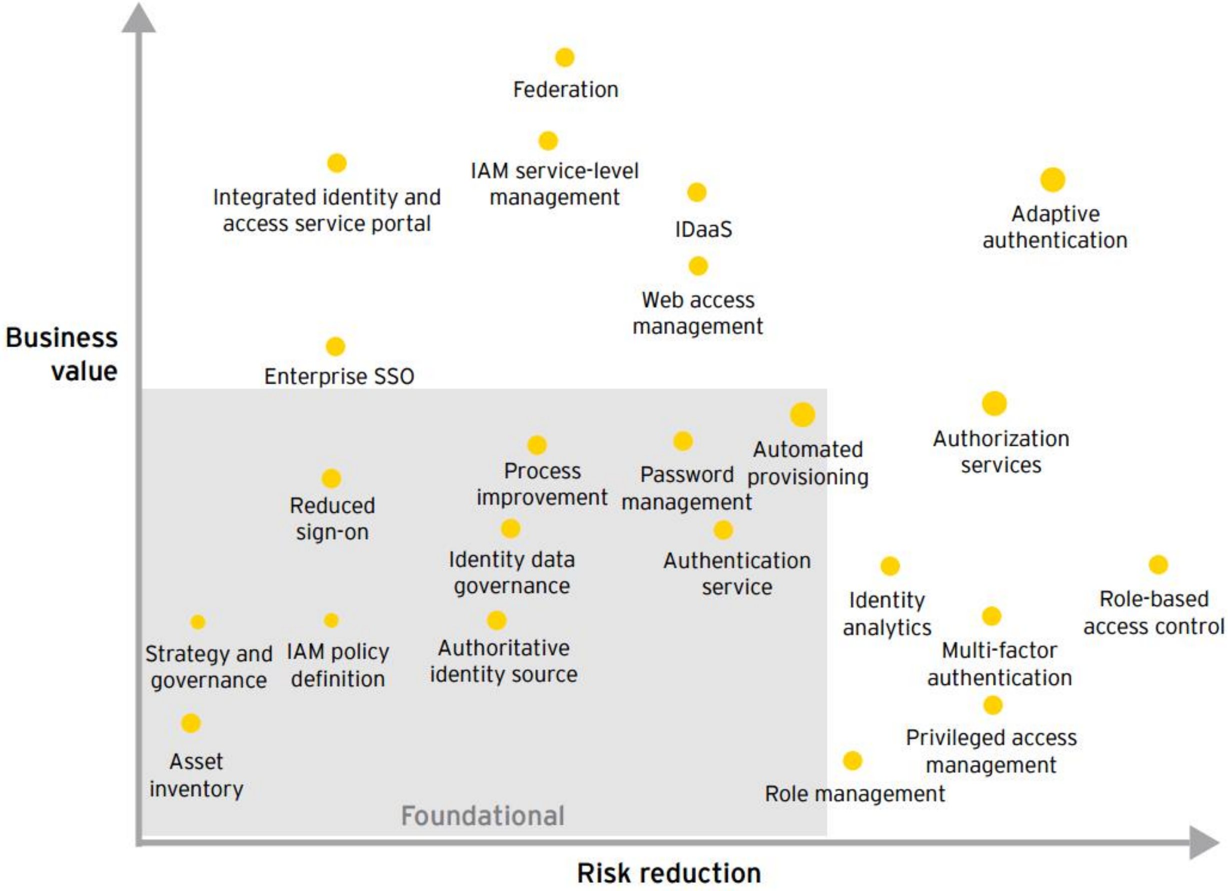
Introduction

- Standarization
  - ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts
  - ISO/IEC 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements
  - ISO/IEC DIS 24760-3 A Framework for Identity Management—Part 3: Practice
  - ISO/IEC 29115 Entity Authentication Assurance
  - ISO/IEC 29146 A framework for access management
  - ISO/IEC CD 29003 Identity Proofing and Verification
  - ISO/IEC 29100 Privacy framework
  - ISO/IEC 29101 Privacy Architecture
  - ISO/IEC 29134 Privacy Impact Assessment Methodology

https://en.wikipedia.org/wiki/Identity_management

Introduction

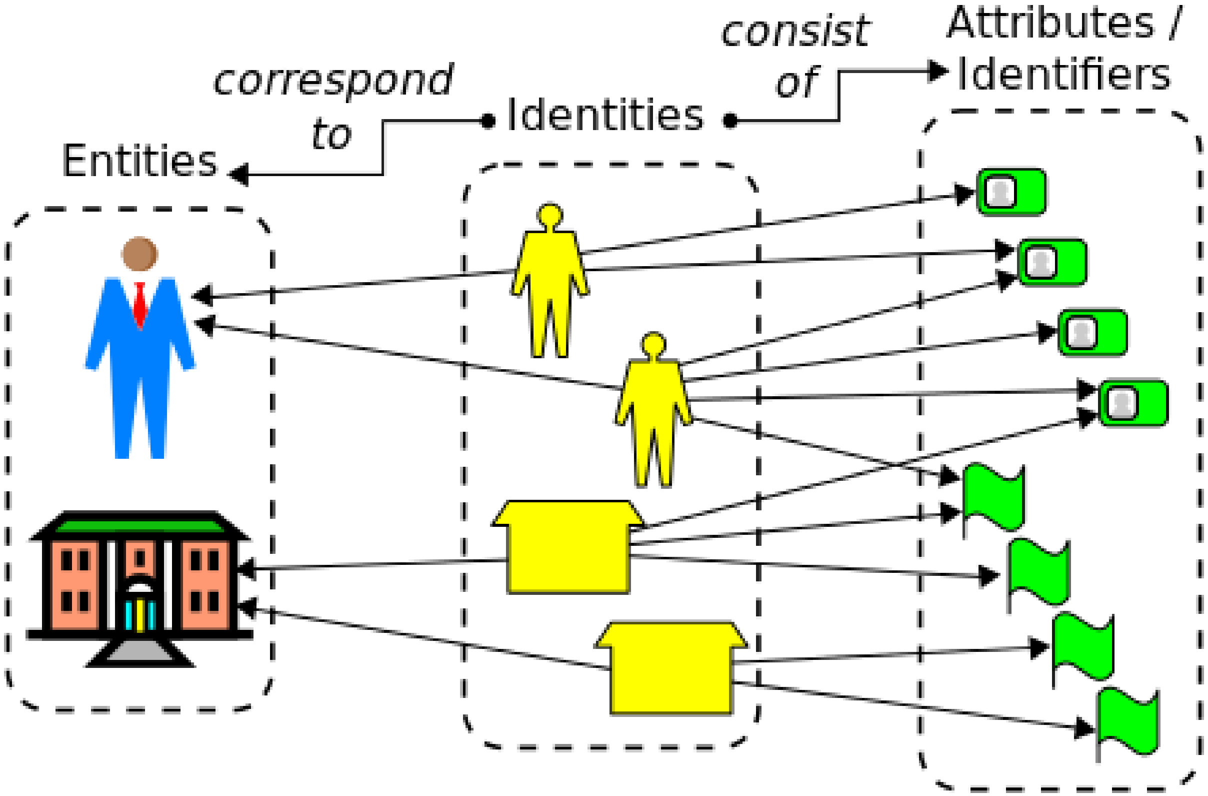
- Business value vs. risk reduction



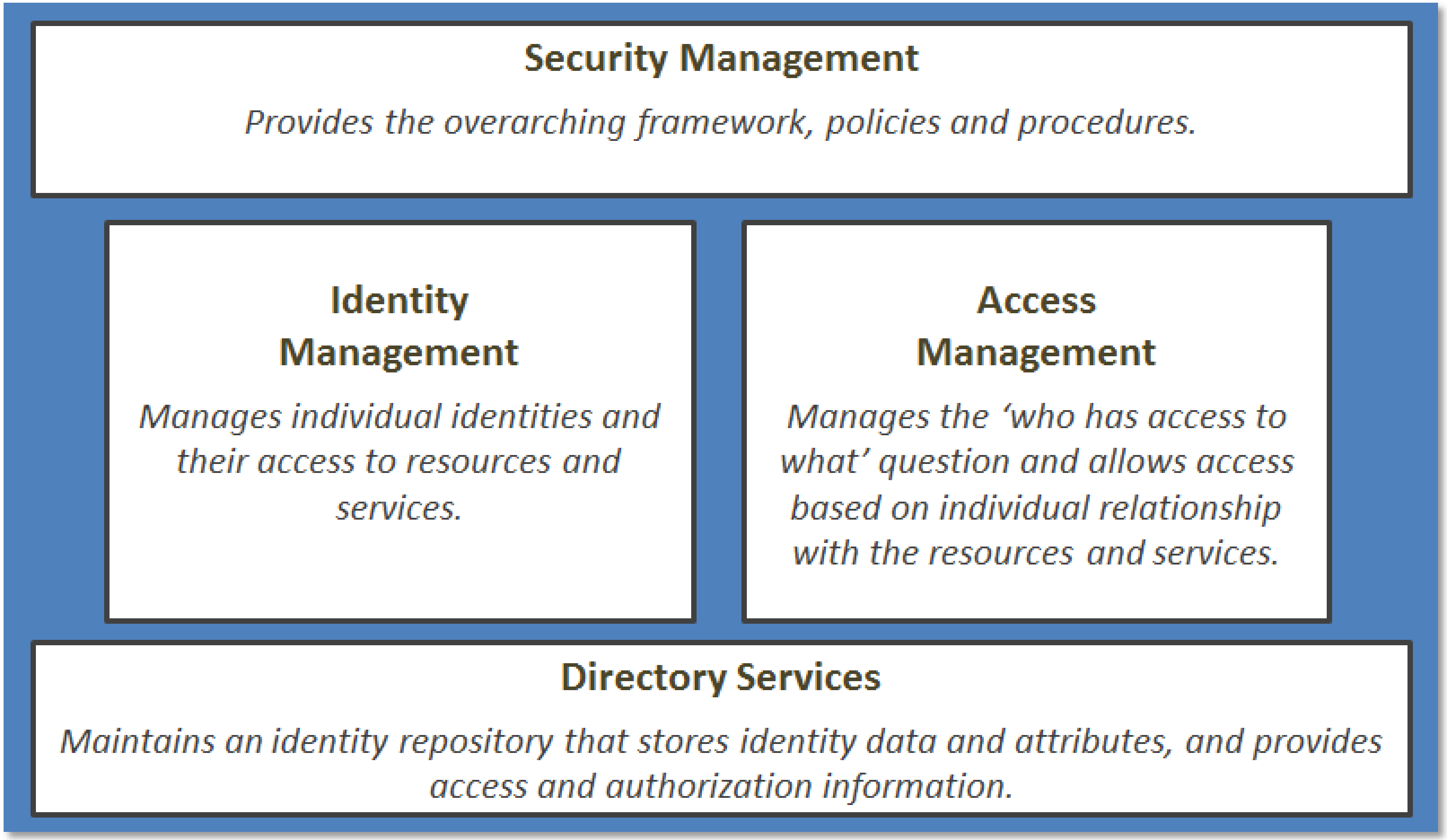
http://www.ey.com/Publication/vwLUAssets/Identity_and_access_management_-_Beyond_compliance/$FILE/Identity_and_access_management_Beyond_compliance_AU1638.pdf

Introduction

- Identities



IAM Processes



Security Management

Provides the overarching framework, policies and procedures.

Identity Management

Manages individual identities and their access to resources and services.

Access Management

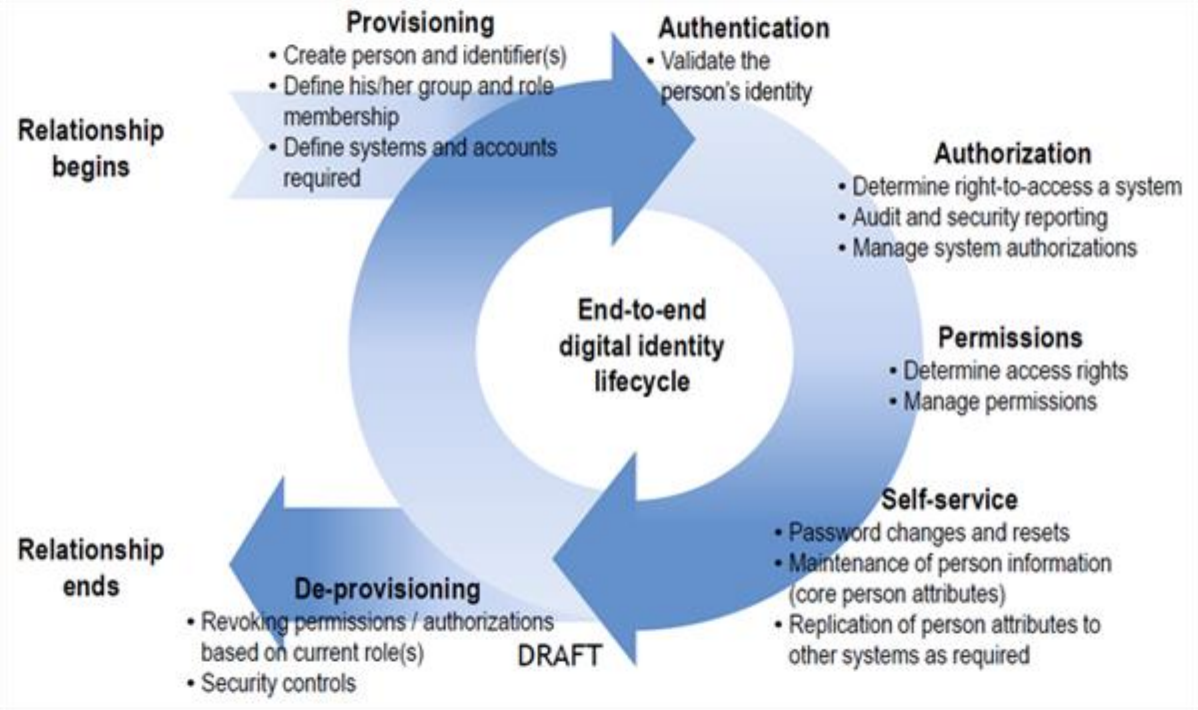
Manages the 'who has access to what' question and allows access based on individual relationship with the resources and services.

Directory Services

Maintains an identity repository that stores identity data and attributes, and provides access and authorization information.

https://www.interfacett.com/blogs/access-management-control-it-just-tools/

IAM Processes



Relationship begins

Provisioning

- Create person and identifier(s)
- Define his/her group and role membership
- Define systems and accounts required

Authentication

- Validate the person's identity

Authorization

- Determine right-to-access a system
- Audit and security reporting
- Manage system authorizations

Permissions

- Determine access rights
- Manage permissions

Self-service

- Password changes and resets
- Maintenance of person information (core person attributes)
- Replication of person attributes to other systems as required

De-provisioning

- Revoking permissions / authorizations based on current role(s)
- Security controls

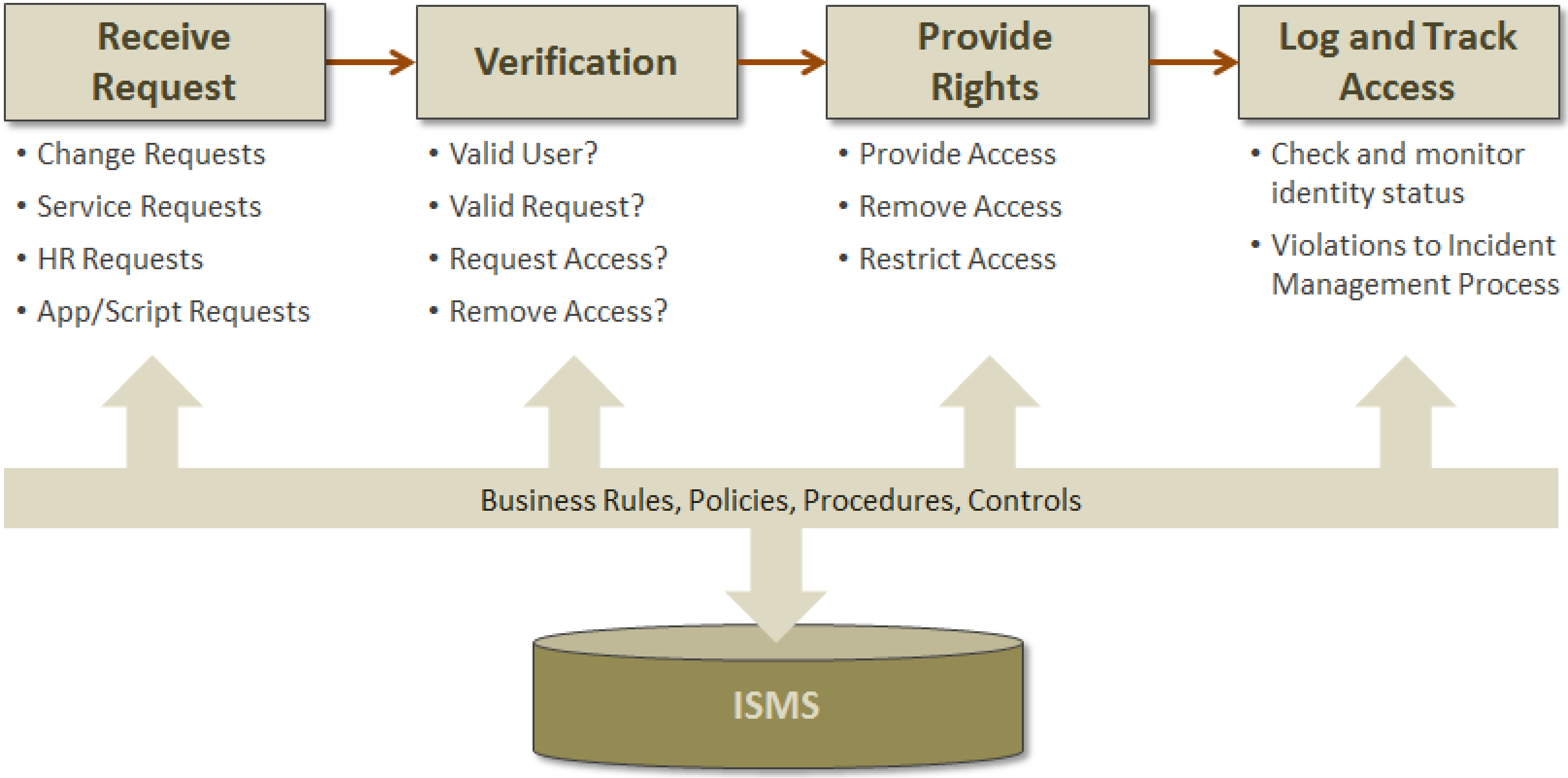
Relationship ends

End-to-end digital identity lifecycle

DRAFT

https://it.ubc.ca/what-identity-and-access-management

IAM Processes



Receive Request

- Change Requests
- Service Requests
- HR Requests
- App/Script Requests

Verification

- Valid User?
- Valid Request?
- Request Access?
- Remove Access?

Provide Rights

- Provide Access
- Remove Access
- Restrict Access

Log and Track Access

- Check and monitor identity status
- Violations to Incident Management Process

Business Rules, Policies, Procedures, Controls

ISMS

https://www.interfacett.com/blogs/access-management-control-it-just-tools/

IAM Services

- Main supporting services
  - Directory services
  - Authentication Services
  - Authorization Services
  - Audit/Accounting Services
  - Token issuer

Directory services: LDAP

- Lightweight Directory Access Protocol
  - Based on X.500 standard
  - Communication over TCP/UDP port 389 (TLS: 636)
  - Hierarchical tree structure
  - Every object in the tree is identified by Distinguished Name (DN)
  - Basic operations:
    - bind, unbind, search, modify, add, delete
  - Every object has defined ACL to control permissions

Directory services: LDAP

- Several basic attributes
  - UID – User Identifier
  - CN – Common Name
  - SN – Surname
  - OU – Organizational Unit
  - O – Organization
  - DC – Domain Component
  - C – Country

Directory services: LDAP

- Searching filter examples

Filter	Meaning
(&(objectCategory=group)(|(cn=Test*)(cn=Admin*)))	Groups with cn starting with "Test" or "Admin"
(&(objectCategory=person)(objectClass=user)(givenName=*)(sn=*))	All users with both a first and last name.
(&(objectCategory=person)(objectClass=user)(pwdLastSet=0))	All users that must change their password at next logon
(&(objectCategory=group)(whenCreated>=20110301000000.0Z))	All groups created after March 1, 2011
(&(objectCategory=computer)(operatingSystem=*server*))	All servers
(member=cn=Jim Smith,ou=West, dc=Domain,dc=com)	All groups with specified direct member

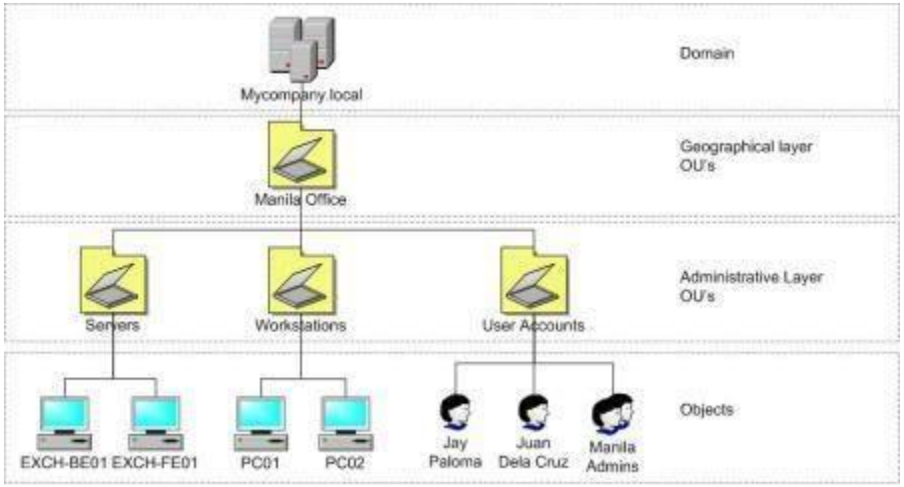
https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

Directory services: LDAP

- The LDAP Data Interchange Format (LDIF)
  - LDAP is a binary protocol
  - LDIF can be used if we want to
    - import and export directory information between LDAP-based directory servers
    - describe a set of changes which are to be applied to a directory
  - RFC: https://tools.ietf.org/html/rfc2849

Directory services: LDAP

- Example structure

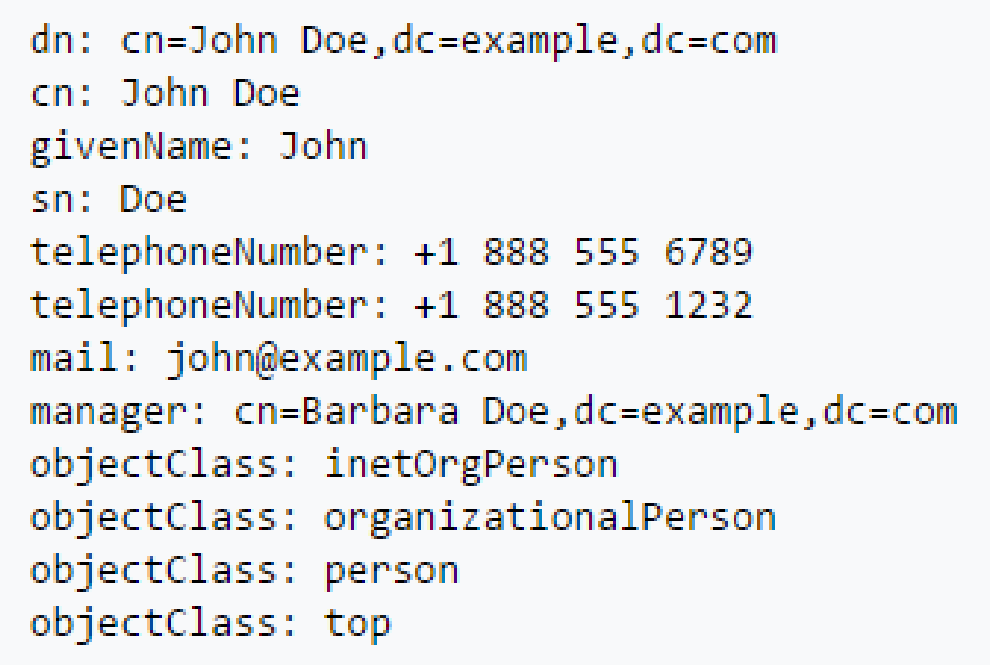


Organizational Units (OU's) are containers that provide the hierarchical mechanism for organizing objects within the domain. OU's can contain user, group and computer objects as well as other OU's

https://jpaloma.wordpress.com/2011/01/19/active-directory-organizational-unit-design-principles/

Directory services: LDAP

- Example entry in LDIF:



```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Directory services: LDAP

- Products on the market
  - Active Directory (Microsoft)
  - Apache Directory Server (Apache Foundation)
  - CA Directory (CA Technologies)
  - IBM Tivoli Directory Server (IBM)
  - NetIQ eDirectory (NetIQ)
  - OpenLDAP (Kurt Zeilenga and others)
  - Oracle Directory Server Enterprise Edition (Oracle)
  - Red Hat Directory Server (Red Hat)

AAA introduction

- Authentication (AuthN)
  - Identification + proof
- Authorization (AuthZ)
  - Permissions is the subject
- Accounting (auditing)
  - Trace information

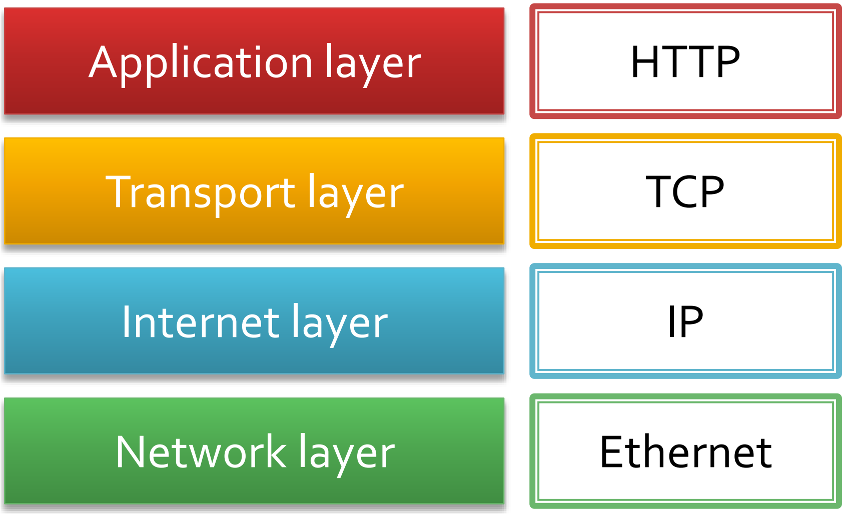
AAA introduction

- Access Control System
  - Combining AAA with additional rules, policies
  - Examples
    - Rules on passwords (complexity, regular changes, history)
    - Object owner is able to determine or define object perms
    - Access denied by default

Authentication

- Purpose
  - Verify a user, verify a service
- Common scenarios
  - User to service
  - Service to user
  - Service to service
  - User to network
  - Service to network

Authentication



Application layer	HTTP
Transport layer	TCP
Internet layer	IP
Network layer	Ethernet

Authentication concepts

- Network level
  - RADIUS
  - TACACS+
- Service level
  - PAP, CHAP
  - HTTP Basic
  - Form-based
  - NTLM
  - Kerberos
  - OpenID Connect (don’t confuse with OpenID)
  - SAML2
  - Smart Cards
    - Includes chip
    - Requires device + PIN
    - Usually combined with multifactor authN

Authentication concepts

- Multifactor authentication
  - Something…
    - you know (e.g. a password)
    - you have (e.g. a token)
    - you are (e.g. a fingerprint)
- Type of authentication
  - Single factor
  - Dual-, multi-factor
    - E.g. smartcard + PIN
    - (password, OTP, PIN, Biometrics)

Authentication concepts

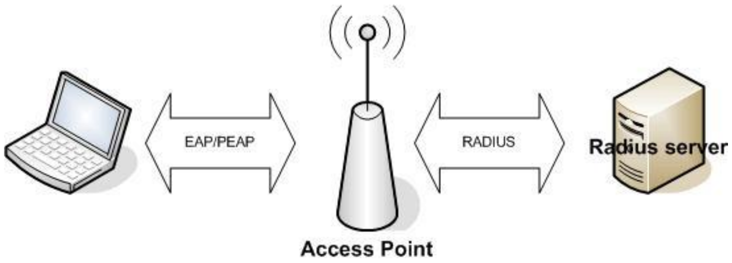
- Single Sign-On
  - Concept
  - Protocols supporting SSO
    - Kerberos, SAML2, WS-Trust, WS-Federation, OAuth2
  - Common solution based on web portals
  - Frequent challenge: cross-domains SSO
- Authentication Services
  - Local
  - Remote

Authentication concepts

- Trunsitive trust (actually, not only authN)
  - One way trust
    - A trusts B / B doesn’t trusts A
  - Two way trust
    - A trusts B / B trusts A
  - Non-transitive trust
    - A trusts B, but doesn’t allow to extend the trust
  - Transitive trust
    - A trusts B, B trusts C, so A trusts C

Authentication methods

- Remote Authentication Dial-In User Service
  - A.k.a. RADIUS
  - Provides AAA capabilities
  - Based on UDP
  - Encrypts only the Password Field
  - Combines Authentication and Authorization
    - Once authenticated RADIUS sends permissions and hand over the control to the network device
  - Primary use: Network Access



http://thebestwirelessinternet.com/radius-server.html

Authentication methods

- Terminal Access Controller Access-Control System
  - A.k.a. TACACS, XTACACS, TACACS+
  - Provides AAA capabilities
  - Based on TCP
  - Encrypts the entire payload
  - Separates Authentication & Authorization
  - Primary use: Device Administration
- There are more, e.g. EAP, 802.1X

http://www.networkworld.com/article/2838882/radius-versus-tacacs.html
http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.pdf

Authentication methods

- PAP
  - Password Authentication Protocol
  - Username/Password is sent to server and verified
  - Password sent in clear text, no longer used
- CHAP
  - Challenge Handshake Authentication Protocol
  - Hash based on shared secret (password) and compared on client and server
  - Used to authenticate PPP clients

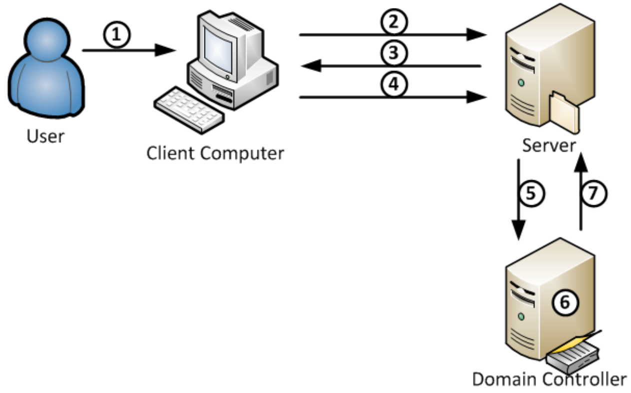
Authentication Methods

- HTTP Basic
  - A client sends a request to a protected resource
  - A server answers with 401 HTTP status
    - Additionaly a Realm (area description) is attached
  - In the client's browser usually a prompt for a login and password pops up
    - With every subsequent request a new header is attached Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
      - In data login:password sequence is encoded using Base64 algorithm
  - After providing a correct credentials the client is able access the resource on the server

Authentication Methods

- Forms authentication
  - Based on login form and authentication cookie
  - Commonly used in simple scenarios
  - HTTPS required
  - Supported in many frameworks

Authentication Methods



- NTLM
  - Challenge/response protocol
  - Versions v1 and v2
  - Not recommended for use, but widely adopted
  - The flow:
    1. A user accesses a client computer and provides:
       domain name, user name, password
       A hash of the password is generated
    2. The client sends the user name to the server (plaintext) (type-1 message)
    3. The server generates a 16-byte random number (challenge/nonce) and sends it to the client (type-2 message)
    4. The client encrypts this challenge with the hash of the user's password and returns the result to the server (response) (type-3 message)
    5. The server sends the following three items to the domain controller:
       - User Name,
       - Challenge sent to the client,
       - Response received from the client
    6. With the username the DC obtain the user's password hash and encrypt the challenge with password's hash.
    7. The DC compares the encrypted challenge it computed (in step 6) to the response computed by the client (in step 4). Based on that authentication is successful or not.

https://blogs.technet.microsoft.com/isrpfeplat/2010/11/05/optimizing-ntlm-authentication-flow-in-multi-domain-environments/

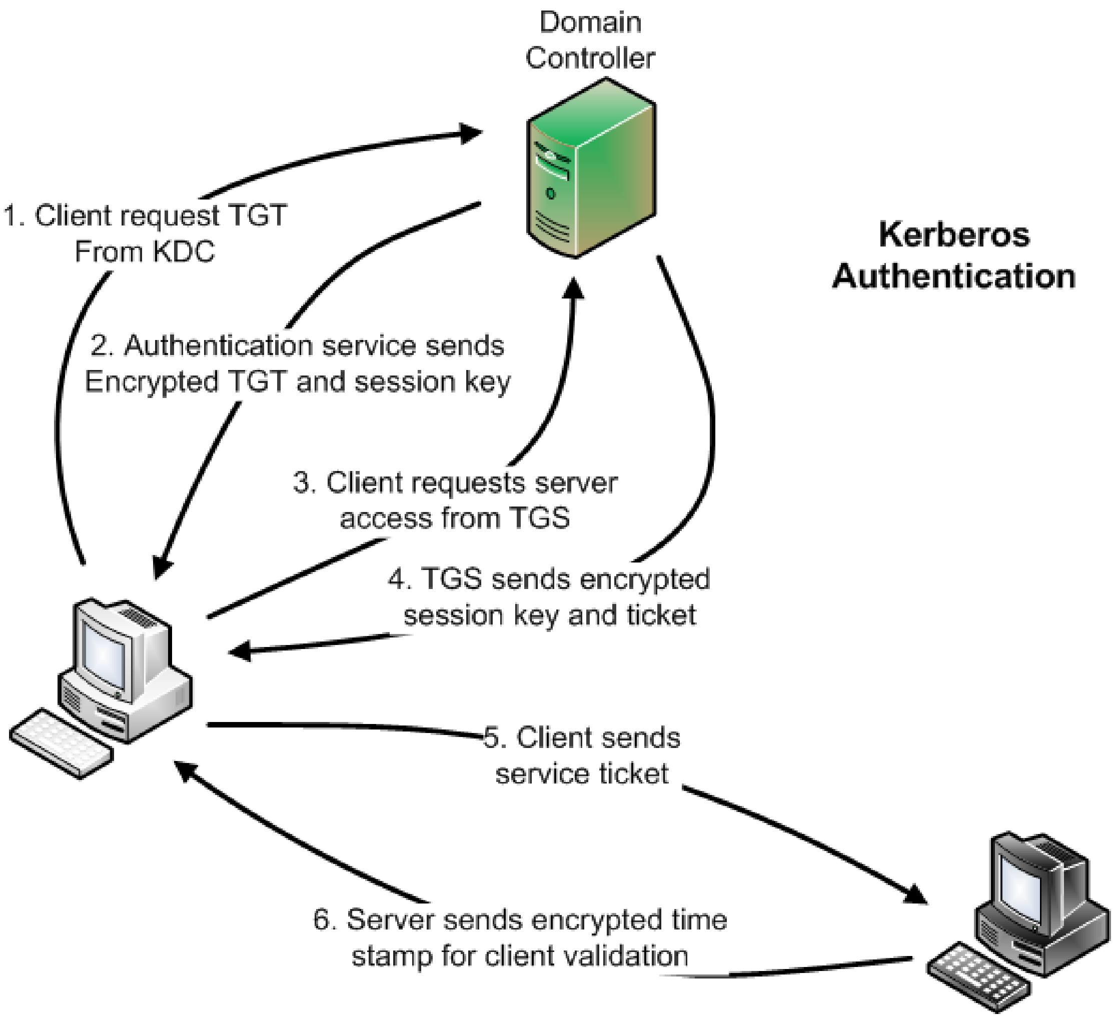
Authentication Methods

- NTLM
  - Flow from Client/Server interaction perspective
    - 1: C → S
      - GET …
    - 2: C ← S
      - 401 Unauthorized
        WWW-Authenticate: NTLM
    - 3: C→ S
      - GET …
        Authorization: NTLM <base64-encoded type-1-message>
    - 4: C ← S
      - 401 Unauthorized
        WWW-Authenticate: NTLM <base64-encoded type-2-message>
    - 5: C → S
      - GET …
        Authorization: NTLM <base64-encoded type-3-message>
    - 6: C ← S
      - 200 Ok

Source: http://www.innovation.ch/personal/ronald/ntlm.html

Authentication Methods

- Kerberos


Domain Controller
Kerberos Authentication
1. Client request TGT From KDC
2. Authentication service sends Encrypted TGT and session key
3. Client requests server access from TGS
4. TGS sends encrypted session key and ticket
5. Client sends service ticket
6. Server sends encrypted time stamp for client validation

Source: *http://digital-forensics.sans.org/blog/2012/09/18/protecting-privileged-domain-accounts-network-authentication-in-depth*

Authentication Methods

- NTLM and Kerberos
  - Headers
    - One can encounter the following headers
      - Authorization: NTLM message-encoded-in-base64
      - Authorization: Negotiate message-encoded-in-base64
    - Of course NTLM means NTLM, however…
    - Negotiate can be both NTLM and Kerberos
  - Kerberos
    - Is faster than NTLM
    - Is an open standard (NTLM not)
    - Supports mutual authN
    - Supports smart card logon
    - Client computer needs to be in the AD domain
  - Read more:
    - http://serverfault.com/questions/254813/why-use-kerberos-instead-of-ntlm-in-iis
    - http://windowsitpro.com/security/comparing-windows-kerberos-and-ntlm-authentication-protocols

Authentication Methods

- OpenID Connect, SAML2
  - Support federation with third party application
  - We will cover that in details in next presentation

Authentication Methods

- CHAP and NTLM are of type CRAM
  - Challenge Response Authentication Method
- CAPTCHA (usually also considered as CRAM)
  - Stands for
    - Completely Automated Public Turing test to tell Computers and Humans Apart
  - Common challenges
    - Finding good ballance (too hard for a user)
    - Applying OCR
    - Social engineering attacks
    - Hire people (e.g. from Asia) to resolve

Authentication factors

- Authentication factors
  - Sth you know
    - Challenge questions
    - Simple/Complex password
    - Swipe gesture
  - Sth you have
    - Certificate
    - OTP (SMS, Digipass)
    - Smart Card
  - Sth you are
    - Fingerprint, retina
  - Where you are
    - Based on location (e.g. GPS)
  - Example combinations
    - Smartcard + PIN
    - Password + OTP
    - Certificate + Password
    - Password + fingerprint

Authentication factors

- Accounts/Passwords – threats
  - Shared/group accounts
  - User can forget the password
  - Weak recovery challenge questions or methods
    - E.g. after 1h discussion you can answer all questions (what a nice dog…)
  - Attacker may see or record when one is typing
  - Keyloggers
  - Stolen passwords database (online vs. offline attacks)
  - Sniffing (e.g. local network)
  - Phishing
  - Dictionary and brute force attack
  - Social attack
  - Re-use attack
    - E.g. the same password in different places

Authentication factors

- Accounts/Passwords – how to protect?
  - Central accounts/passwords management (AD)
  - Policy enforcement for whole domain
  - Encrypt or hash passwords
  - Apply salt and pepper for hashes (why?)
  - Don’t use default accounts (admin, guest)
  - Smart policy in case authentication failed
    - Lock after 6 tries (is it a good idea?)
    - 3s delay to the next try

Authentication factors

- Accounts/Passwords – how to protect?
  - Password policy
    - Complexity
      - Password vs. passphrase
      - Specials chars, upper/lower
    - Expiration (when by default?)
    - Minimum length
      - Do we really need 16 characters long passwords? Why PINs are only 4 digits long?
    - Password history
      - With minimum time of usage – why?
  - Masked password
  - Remember password (ORLY?)

Authentication factors

- Smart cards – threats
  - Steal card
  - Hack an issuer of cards
- One-time passwords – threats
  - We consider both
    - Synchronic (generators on both sides)
    - Asynchronic (challenge-response protocol)
  - Again, steal device, hack device
  - Find a initial value for generator
    - Through hacking an issuer server

Authentication factors

- Biometrics – threats
  - Retina scan, finger print, voice recognition, signature recognition
  - Main problem: biometrics accuracy
    - False Rejection Rate (FRR) – false negative
    - False Acceptance Rate (FAR) – false positive
  - Accuracy problem implies that one may pretend by getting e.g. victims fingerprints
  - Accuracy ranking
    - retina > fingerprint > signature > voice

Authorizations

- Define who is allowed to do what
  - Very often expressed as a matrix
- Make sure they are documented, consistent and complete
- Put special attention to privileged and administrative accounts
- Authorizations can be
  - very simple (expressed by roles)
  - very complicated (with business logic)
- Related area: authorizations management

Accounting

- Mechanism to trace activities in the solution
- Can be local or centralized
- Usually mandatory for priviliged and admin accounts
- What to trace?
  - Login attempts (successful or/and not)
  - Modification of records
  - Reads of records
  - Many others (should be defined in policies & directives)
- Challenges
  - Strategy for log retention
  - Make sure that log is protected
  - No repudiation

Access Control

- Combining AAA with additional policies
- Execute check if a subject should access the resource or activity
- Usually we consider
  - Decision Point
  - Enforcement Point
- Role of „jump-host”
- Common pricinples
  - Least privilege, Need to know
  - Separation of duties
    - Prevents one person get to much power
    - Can be defined on the permissions level
- Time of day restrictions

Access Control Models

- Discretionary Access Control
  - Owner of an object is able to decide who is allowed to access it
  - Very flexible, but less secure
  - Common example: file system ACL
- Mandatory Access Control
  - Access rules defined centrally
  - Inflexible and hard to manage
  - … but offers the higher security
  - Usually based on hierarchical sensitive labels

Access Control Models

- Role-based access control
  - Based on roles/groups
  - Roles are usually organized in a hierarchy
  - Roles are controlled centrally
    - MAC model is intended for only read and write
    - Roles are considered as set of permissions and give more flexibility
  - A lot of systems implement RBAC
- Attribute-based access control
  - Not based on rights assigned to subject
  - Based on attributes which are used to prove the truth of statements (i.e. claims)
  - Example:
    - Claim: „older than 18"
    - Anyone, who can prove that statement, has granted access

Source: http://en.wikipedia.org/wiki/Computer_access_control

Access control solution

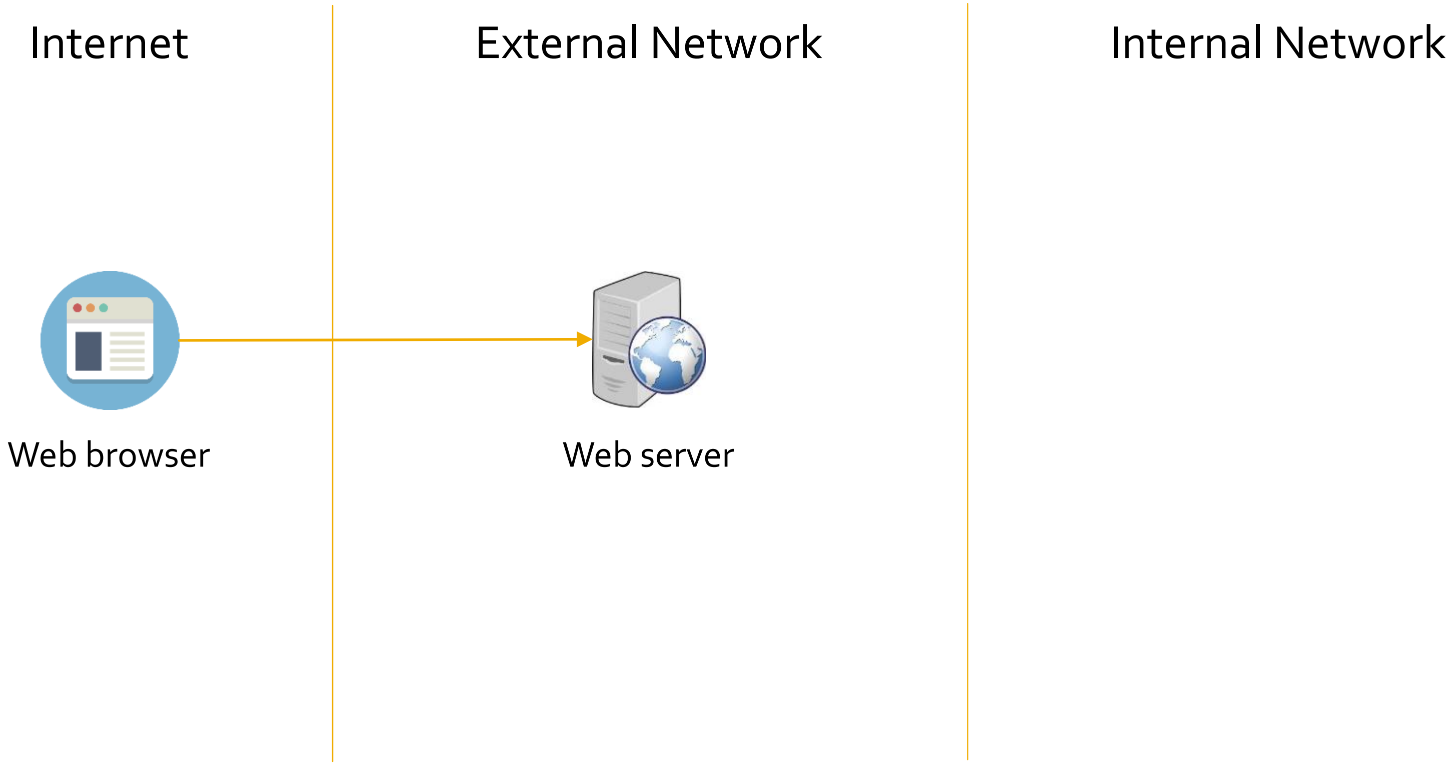
- Access control in software architecture

User Interface	Adjust web controls, optionally EP
Application Services	Mandatory EP
Domain	Authorization logic, service in every Bounded Context (central service to consider, usually not possible)
Infrastructure	EP if needed, depending on requirements

- Consider CQS

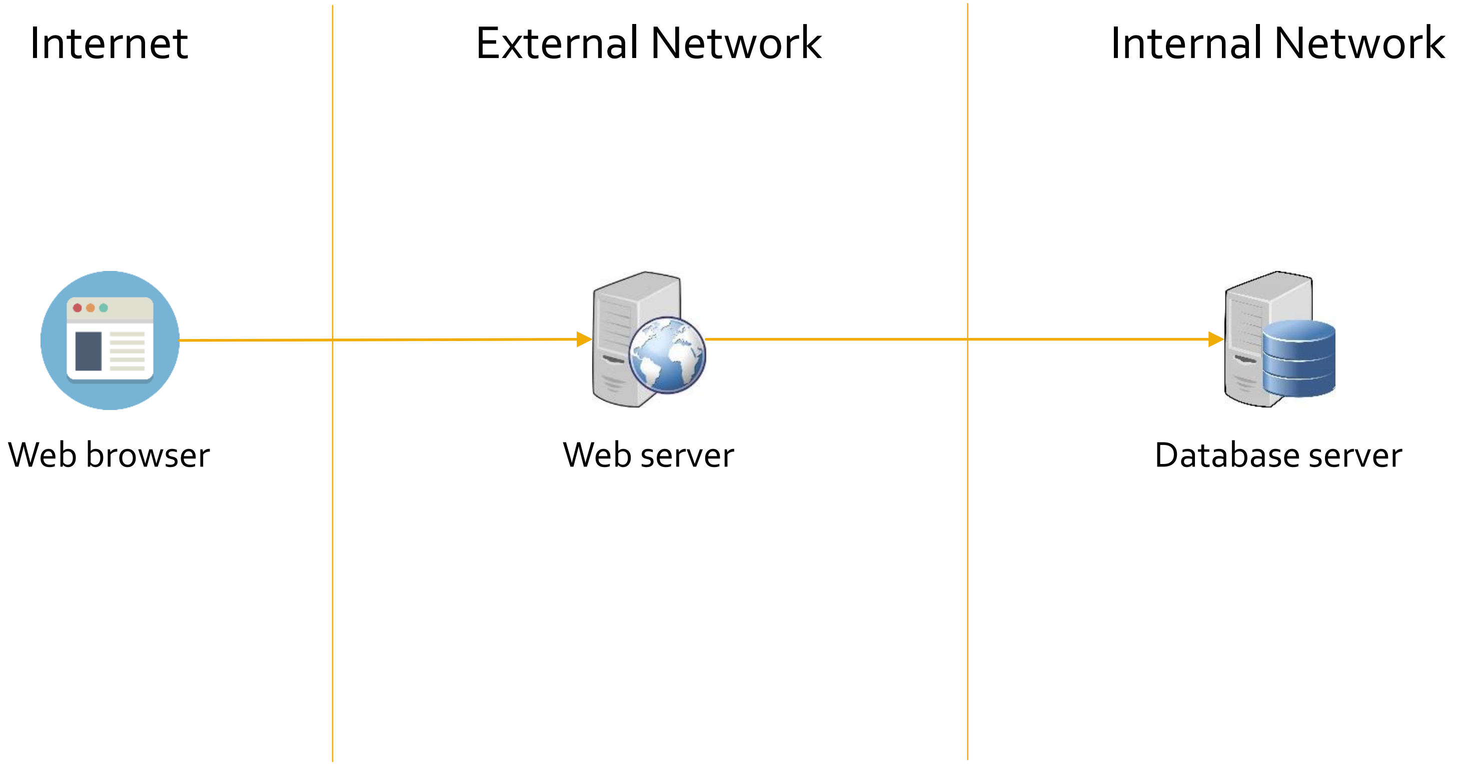
Access control solution

- Simple scenario



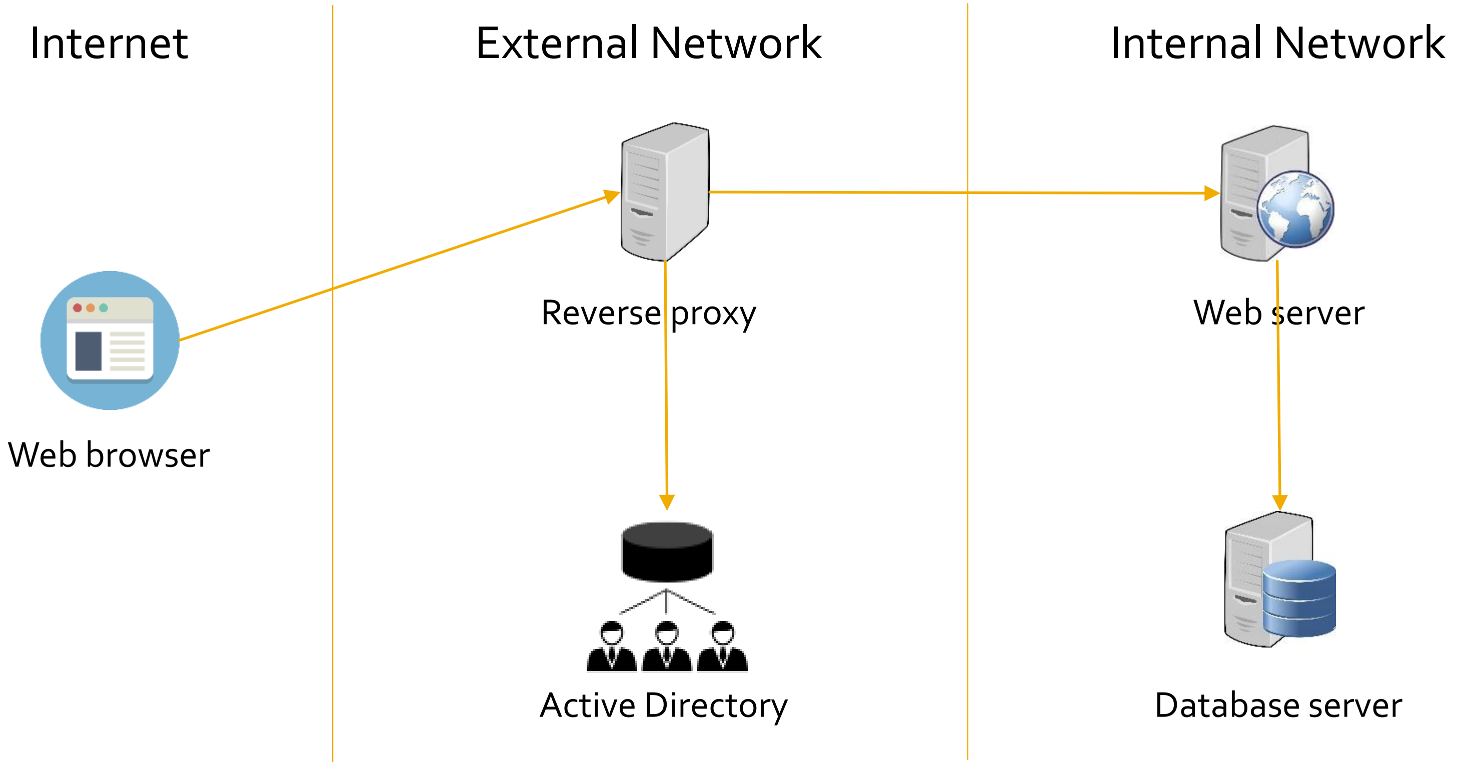
Access control solution

- Simple scenario with a database



Access control solution

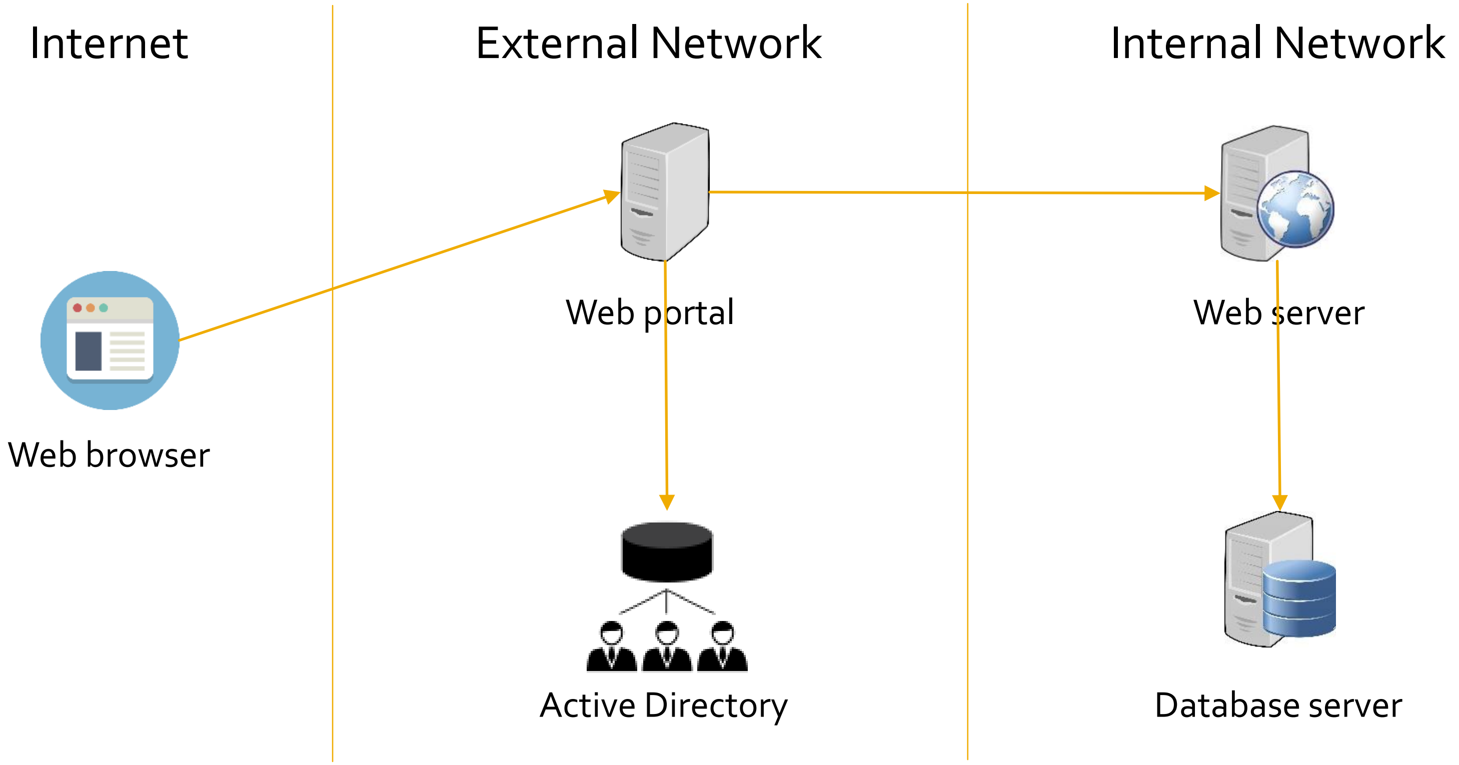
- Scenario with a reverse proxy



Q: Where is the EP? What is the split between Reverse Proxy and Web server? Role of Web Access Management

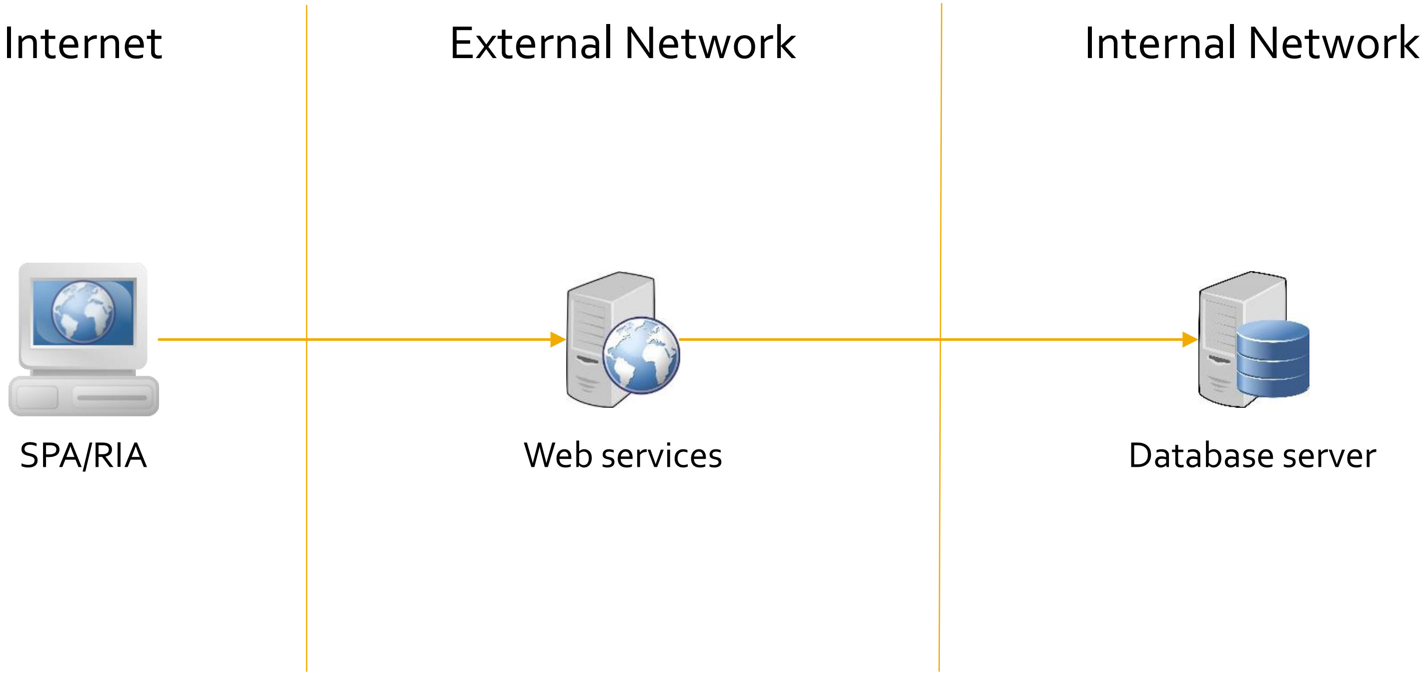
Access control solution

- Scenario with a web portal (including SSO)



Access control solution

- Simple scenario with a SPA/RIA



Q: What if client needs to support offline mode?