Cyber Security Morning

Securing confidential information with Identity Access Management

Kari Nousiainen & Laura Karintaus

20.2.2020

metso

Information Access Governance

- Why: We want to ensure that important information assets (eg IP) are accessed only by the appropriate persons and protect information from being used wrong

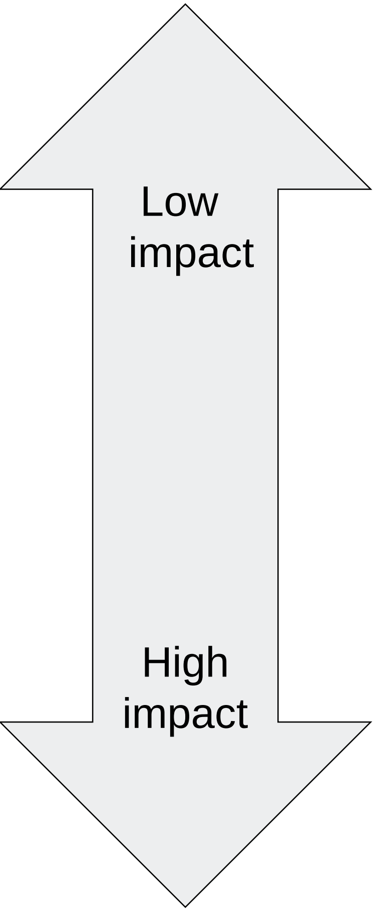
- Access controls to confidential information will be based on IAM assurance levels.
  - An IT system can hold different levels of confidential information.

- Access decisions to be made by Data Owners and Custodians.
  - Persons in the business area/group function owning the data.

- Company-wide IAM governance model
  - Its purpose is to oversee identity and access management processes and to prioritize the IAM tasks and goals.

Assurance levels for accessing confidential information

Minimum requirements to be used based on the business impact

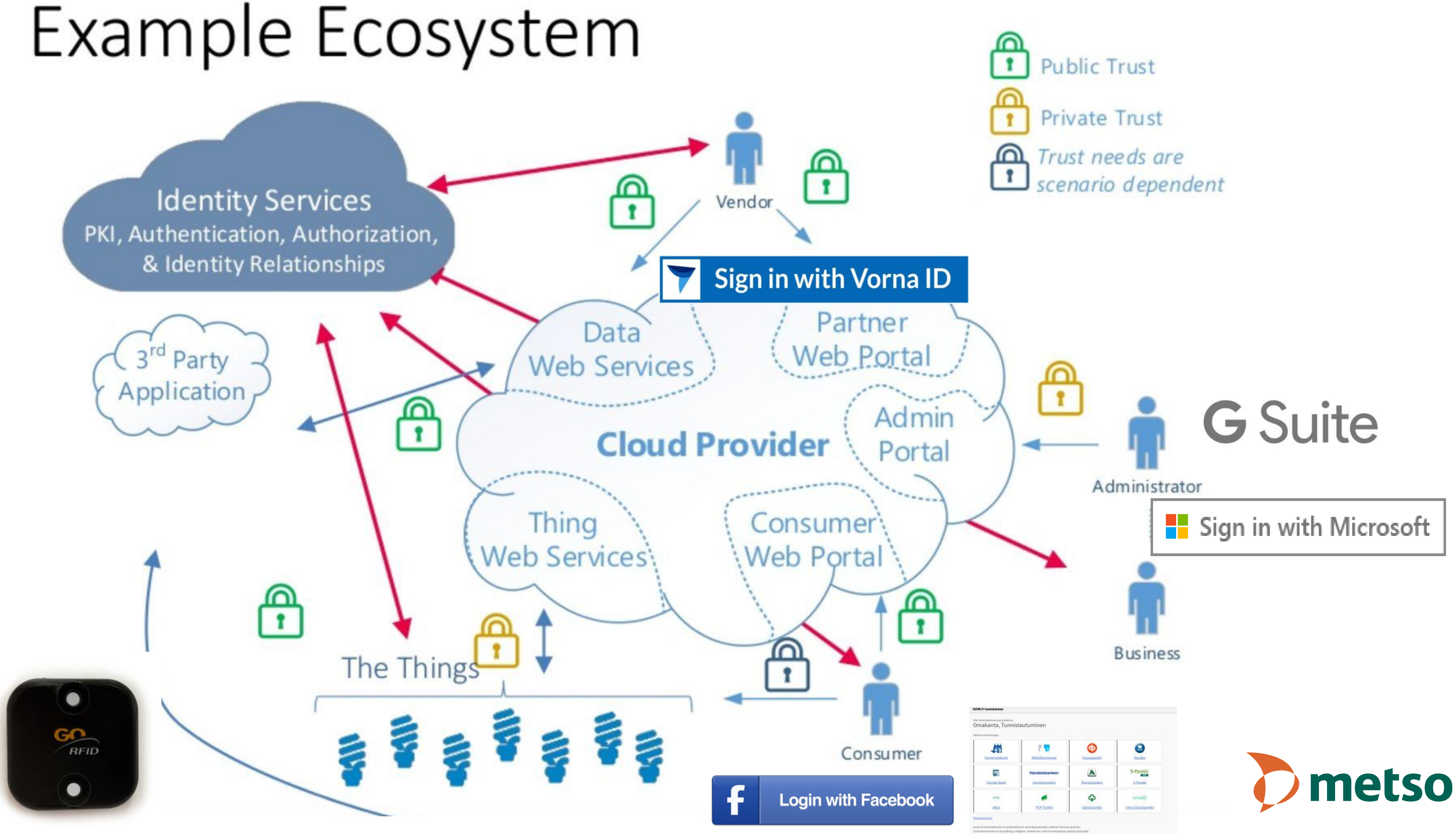


Low impact

High impact

Assurance Level	Authentication Assurance (with session limits)	Authorization Assurance (with access certification)	Identity Assurance	Federation Assurance
1 (Restricted)	Single-factor authentication	Based on contractual relationship (with business roles)	Verified e-mail	Bearer assertion, signed by IdP and encrypted to RP
2 (Confidential)	Multi-factor authentication	Manual approval by person’s manager or data owner	In-person or remote vetting	Same as Level 1
3 (Secret)	Multi-factor authentication with hardware token	Manual approval by person’s manager and data owner	In-person (to include supervised remote) vetting	Holder of key assertion, signed by IdP and encrypted to RP

Example Ecosystem



SUOMI.FI-tunnistaminen

Olet tunnistautumassa palveluun

Omakanta, Tunnistautuminen

Valitse tunnistustapa

Varmennekortti	Mobiilivarmenne	Osuuspankki	Nordea
Danske Bank	Handelsbanken	Ålandsbanken	S-Pankki
Aktia	POP Pankki	Säästöpankki	Oma Säästöpankki

Palaa palveluun

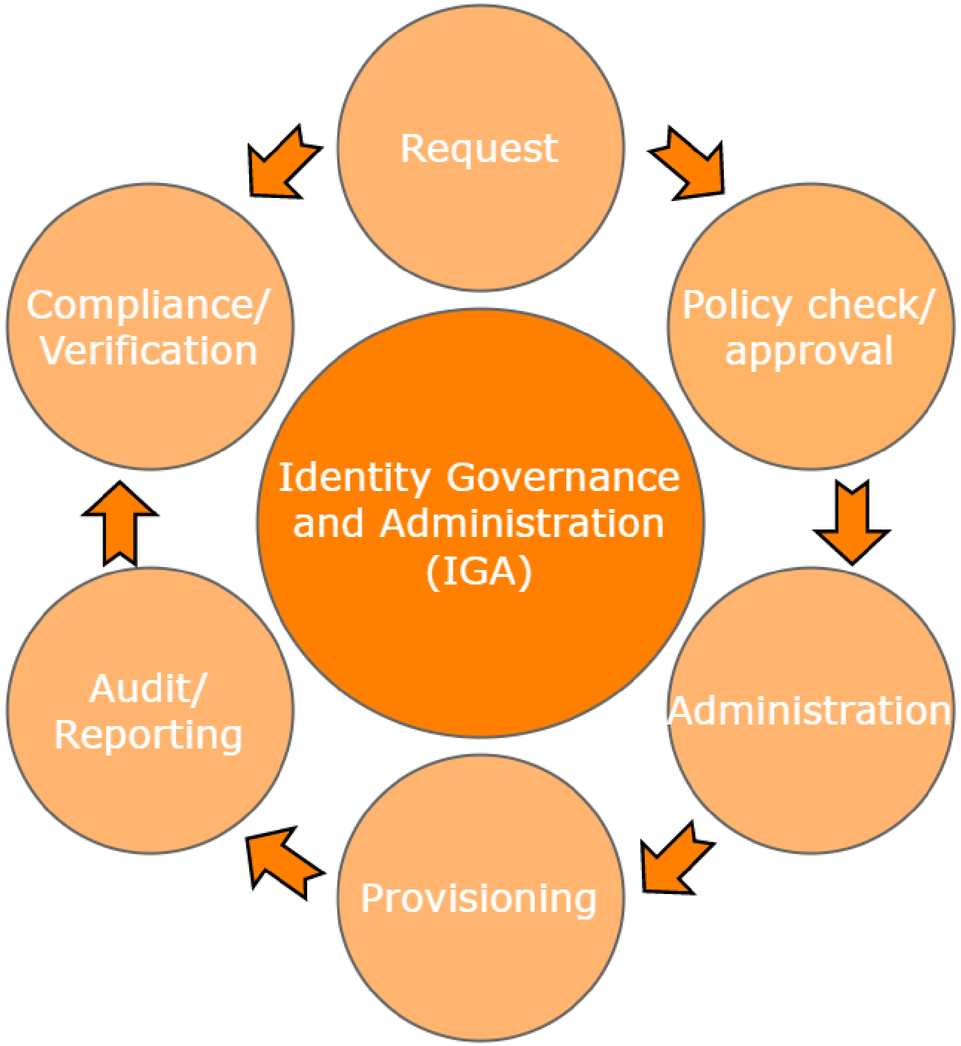
Suomi.fi-tunnistaminen on julkishallinnon asiointipalveluiden yhteinen tunnistuspalvelu. Tunnistautuminen on turvallista ja helppoa. Valitset itse, mitä tunnistustapaa haluat hyödyntää.

Creating governance model

Laura Karintaus

From IAM to IGA

- IAM focuses mainly on user provisioning and individual systems
- In IGA: supervision, governance and processes are also included
- IGA provides visibility into information assets over individual systems



IGA development phases

- Current-state-study with IAM Partner

- Discussions with IGA-product suppliers and their customer references
  - Piloting the chosen solution with selected business area

- Identifying all information assets and responsibilities
  - Unifying Processes – Providing uniform data to work with
  - Increasing Visibility – Building on what we see
  - Detecting and Automating – Getting actionable insights on data changes

Roles in Authorization Process

- Data Owners (Mostly in business)
  - Data Owners must make decisions regarding the handling of data in accordance with the Information Security Guidelines and Information Classification and in compliance with all relevant laws and regulations.

- Data Custodians (Mostly in IT)
  - These individuals are responsible for executing the approved account definition/modification/removal request, after validating that appropriate approvals have been granted.

- IAM Process Owner/Specialist (IT Security)
  - Accountable to internal control for the proper design, execution, and improvement of the access process. This individual ensures that the process is being carried out, but does not run the day-to-day operation of the process.

Questions?

metso

Expect results

www.metso.com

company/metso metsoworld metsogroup metsoworld metsogroup