Weak and strong passwords

When to use them and how to protect them

Prof Audun Jøsang

Department of Informatics
University of Oslo

Authentication Assurance Requirement

Service sensitivity

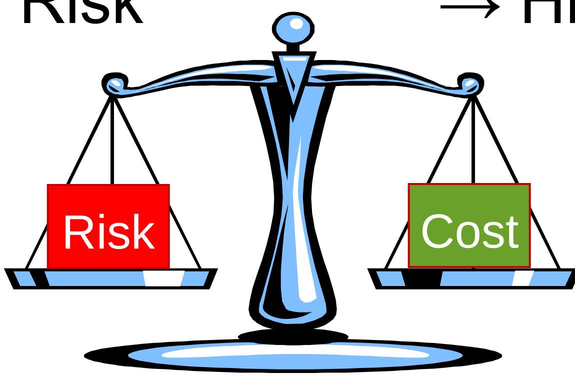
Higher Sensitivity

→ Higher Risk

Authentication cost

Stronger Authentication

→ Higher Cost



- Authentication assurance should reflect application sensitivity.
- Risk of getting e-Authentication wrong must balance the cost.

Authentication Assurance Levels

Example taken from Australian NeAF 2009

No Assurance	Minimal Assurance	Low Assurance	Moderate Assurance	High Assurance
Level 0	Level 1	Level 2	Level 3	Level 4
No registration of identity required	Minimal confidence is required in the identity assertion	Low confidence is required in the identity assertion	Moderate confidence is required in the identity assertion	High confidence is required in the identity assertion

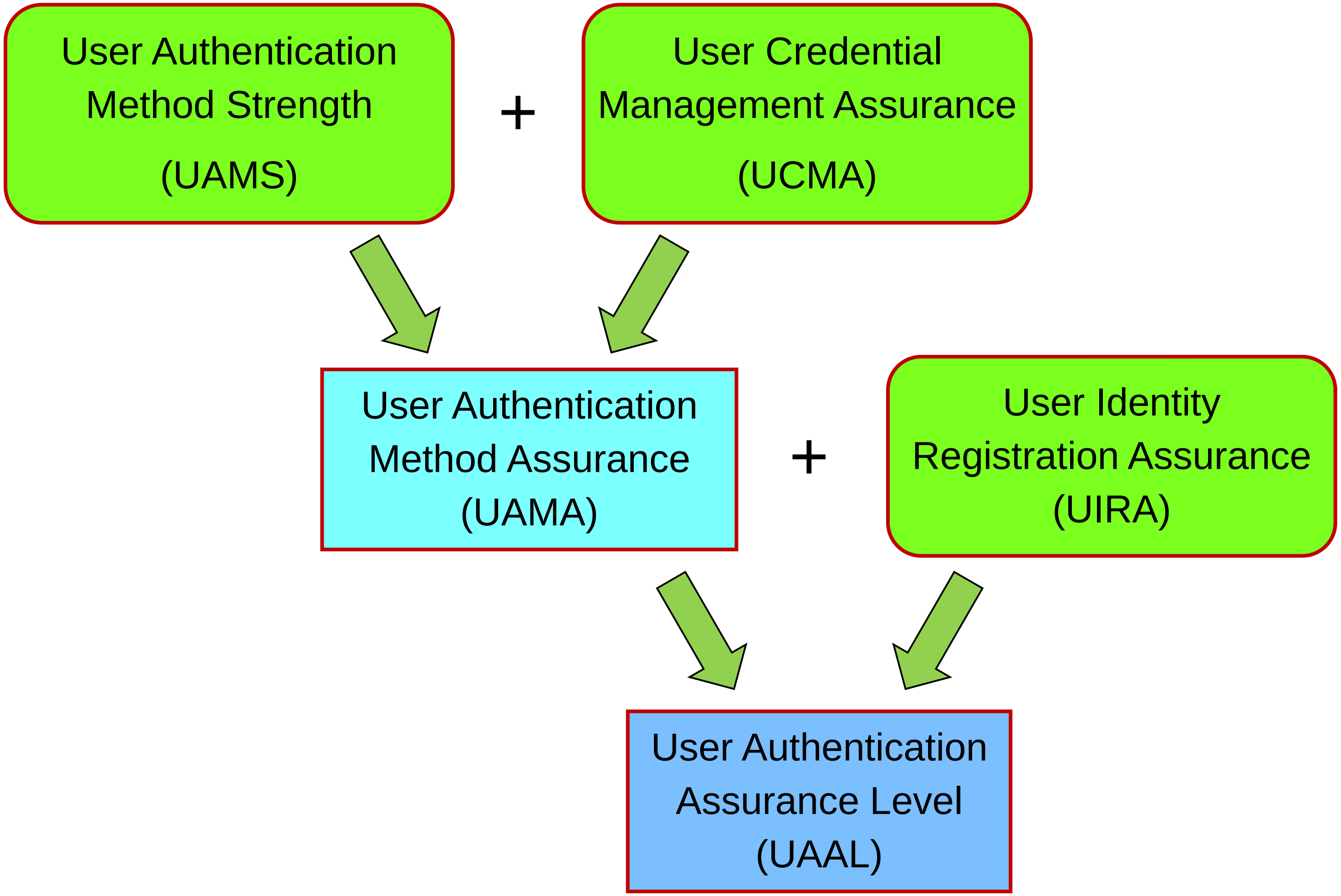
Authentication Assurance Levels

- AAL-1
  - typically used when users self-register, meaning that it is not important to verify that registered identity corresponds to true identity.
  - e.g. online free subscription
- AAL-2
  - Typically used when the SP wants to verify that registered identity corresponds to true identity
  - Consequences associated with false identity are still relatively low, which reduces the level of authentication assurance required.
  - e.g. online paid subscription

Authentication Assurance Levels

- AAL-3
  - Typically used when true identity required
  - Consequence of false identity is significant, thereby requiring relatively strong authentication assurance.
  - e.g. online banking
- AAL-4
  - Typically used when true identity required
  - Consequences of false identity could be very high, thereby requiring the highest level of authentication assurance.
  - e.g. online election

User Authentication Assurance Factors



User Authentication Frameworks

Authentication Framework	***User Authentication Assurance Levels***				
NIST (USA) 2006	Little or no assurance (1)		Some (2)	High (3)	Very High (4)
IDABC (EU) 2007	×	Minimal (1)	Low (2)	Substantial (3)	High (4)
FANR (Norway) 2008	Little or no assurance (1)		Low (2)	Moderate (3)	High (4)
NeAF (Australia) 2009	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)
NeAF (India) 2011	None (0)	Minimal (1)	Minor (2)	Significant (3)	Substantial (4)

Password requirements for AAL-1

- **NIST (USA):** Probability of success of a targeted on-line password guessing shall not exceed 2^{-10} (1 in 1024), over the life of the password. There are no min-entropy requirements for Level 1. Passwords must never be transmitted in clear.
- **IDABC (EU):** Password or PIN token can be chosen by the claimant.
- **FANR (NO):** Password can be self-chosen password, and can be transmitted in clear over network.
- **NeAF (AU):** Can be based on memorized password, or or a list of passwords (code book), where both types must have a minimum entropy.

Password requirements for AAL-2

- **NIST (USA):** Probability of success of an on-line password guessing attack shall not exceed 2^{-14} *(1 in 16,384),* over the life of the password. At least 10 bits of min-entropy, never be transmitted in clear.
- **IDABC (EU):** Randomly generated password, PIN token or password list (but not passwords or PIN tokens chosen by the claimant).
- **FANR (NO):** Generated static or dynamic passwords (e.g. pre-computed list or unprotected OTP calculator).
- **NeAF (AU):** Memorized password, or list of passwords (code book), both with minimum entropy. Blocked account after a specific number of successive invalid passwords.

Password requirements for AAL-3

- **NIST (USA):** Requires 2-factor authentication, where an OTP device can represent the 1st factor. The OTP output by the device shall have at least 106 possible values. The 2nd factor can be one of:
  - *Authentication mechanism used to authenticate the claimant to the token, e.g. PIN or biometric.*
  - *The claimant sends the verifier (the hash of) a personal static password meeting the requirements for (E-authentication) Level 1 together with the one-time password. Personal static passwords must not be sent in clear.*

  In addition, the verifier must be authenticated cryptographically to the claimant, e.g. with TLS.

Password requirements for AAL-3

- **IDABC (EU):** Requires 2-factor authentication, where 1st factor can be software or hardware based OTP generator. Static password not acceptable as 2nd factor.
- **FANR (NO):** Requires 2-factor authentication, where a static password and a list of static passwords (both generated by verifier) can represent one or both factors.
- **NeAF (AU):** Requires 2-factor authentication, e.g. list of generated passwords (code book) with minimum entropy, combined with authentication code diversification through shared secret.

Password requirements for AAL-4

- **NIST (USA):** Requires 2-factor authentication. Personal static passwords are **not** acceptable as a factor.
- **IDABC (EU):** Requires 2-factor authentication. Personal static passwords are **not** acceptable as a factor.
- **FANR (NO):** Requires 2-factor authentication, where the 1st factor must be asymmetric cryptographic hardware. The 2nd factor can be a generated static password or dynamic password (e.g. from protected OTP device).
- **NeAF (AU):** Requires 2-factor authentication. Personal static passwords are **not** acceptable as a factor.

Surveyed password policies

Service	Length	Char. Sets	Chg. fr. months	Assumed AAL
Wikipedia	≥ 1	-	-	AAL-1
NY Times	5-15	-	-	AAL-1
QUT	≥ 8	= 4	2	AAL-2
Oslo Uni	≥ 8	≥ 3	11	AAL-2
eBay	≥ 6	≥ 2	-	AAL-2
CitiBank	≥ 6	≥ 2	2	AAL-3
Nordea Bank	≥ 6	-	12	AAL-3
Samba Bank	≥ 8	= 3	-	AAL-3
SANS Policy	≥ 15	≥ 3	3	AAL-2,3

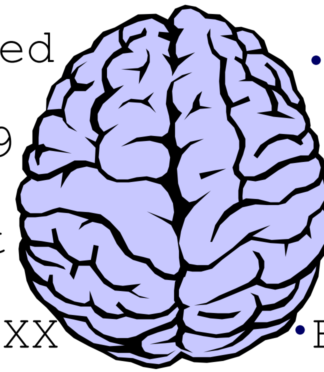
4 password policies to Rule them all

AAL	Length	Character Sets	Restric-tions
AAL-1	≥ 6	-	-
AAL-2	≥ 8	≥ 2	No-reuse
AAL-3	≥ 13	≥ 3	No-cache
AAL-4	≥ 15	$= 4$	No-expose

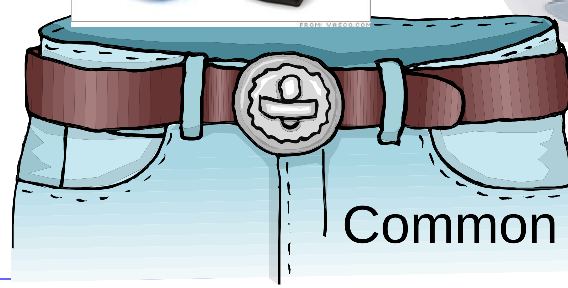
Tragedy of the Commons

Common village grazing field

- Password1
- fred
- 123456
- 2008Oct9
- MySecret
- TopSecret
- XZ&9r#/
- ???abcXX
- FacePass

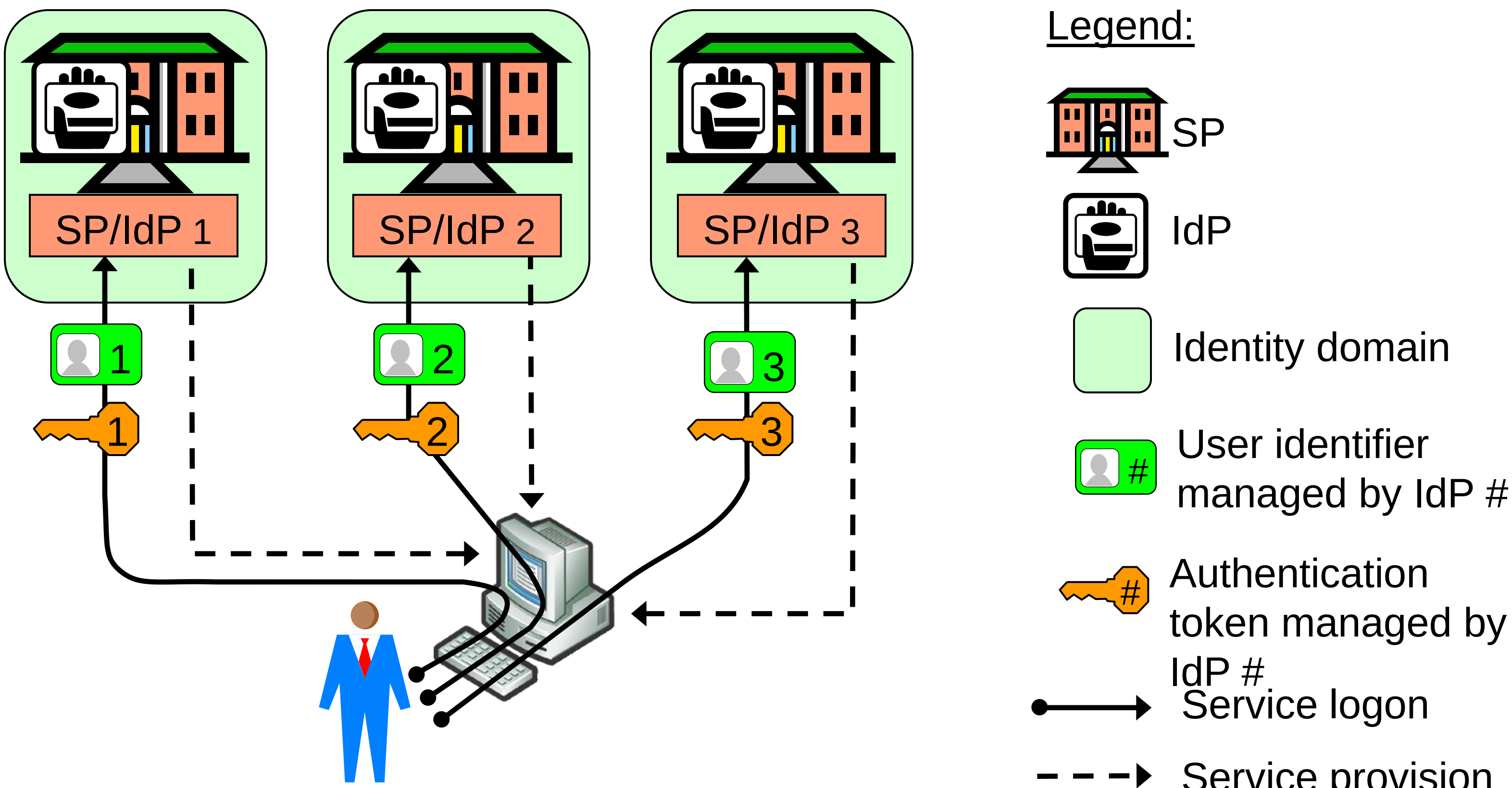


Common brain



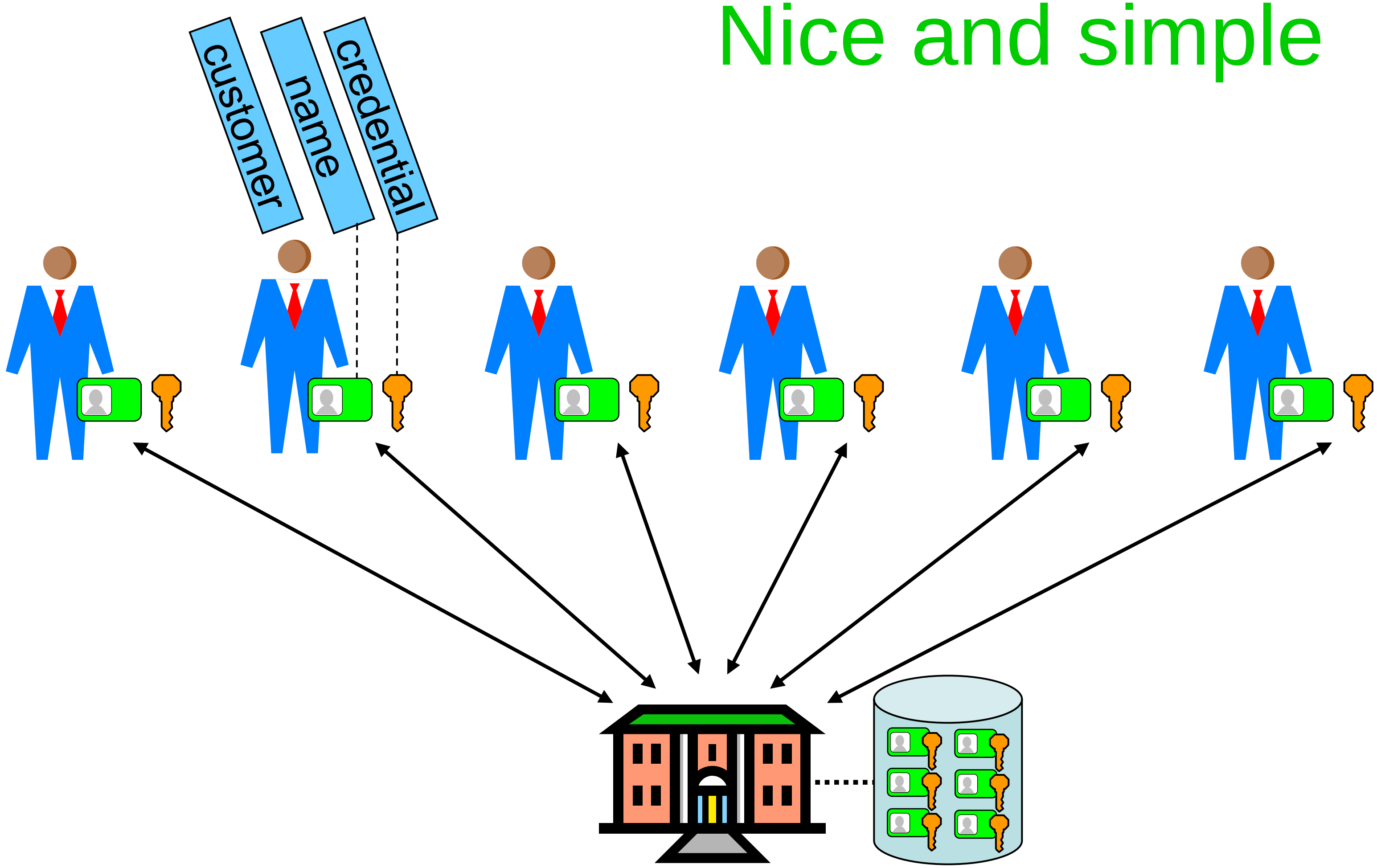
Common pockets

Silo domain model



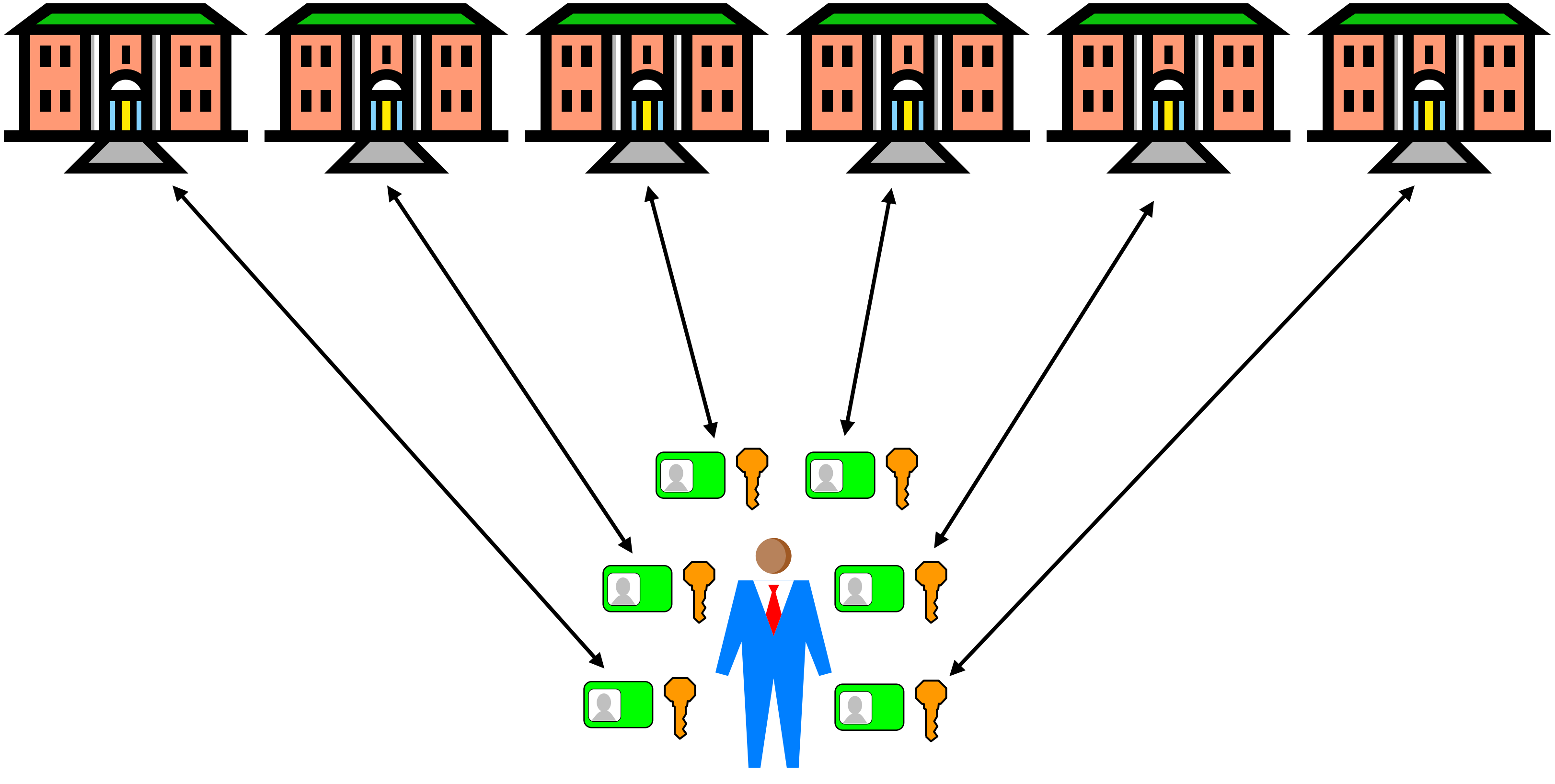
Imagine you're a service provider

Nice and simple

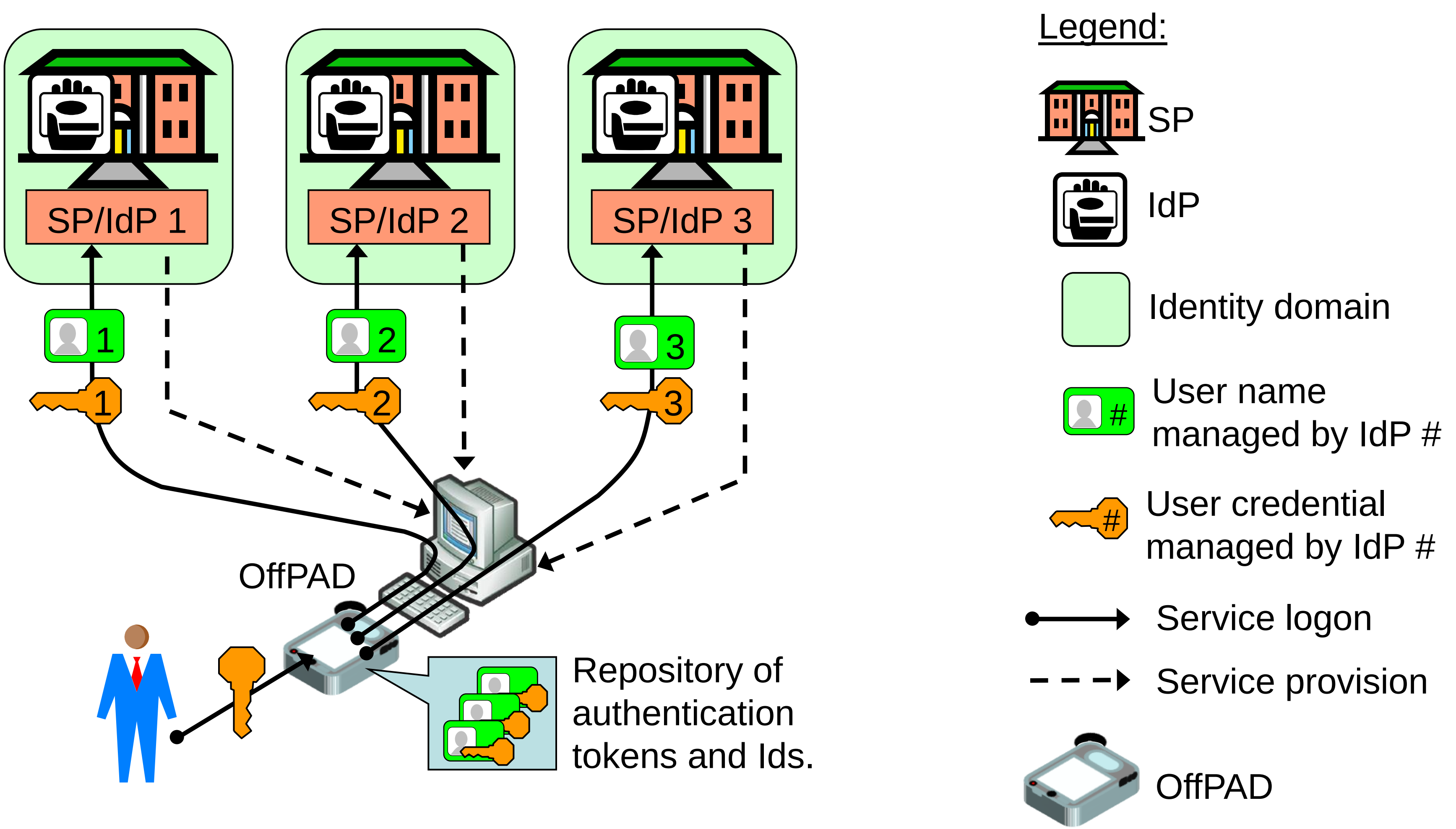


Imagine you're a customer

It's a nightmare

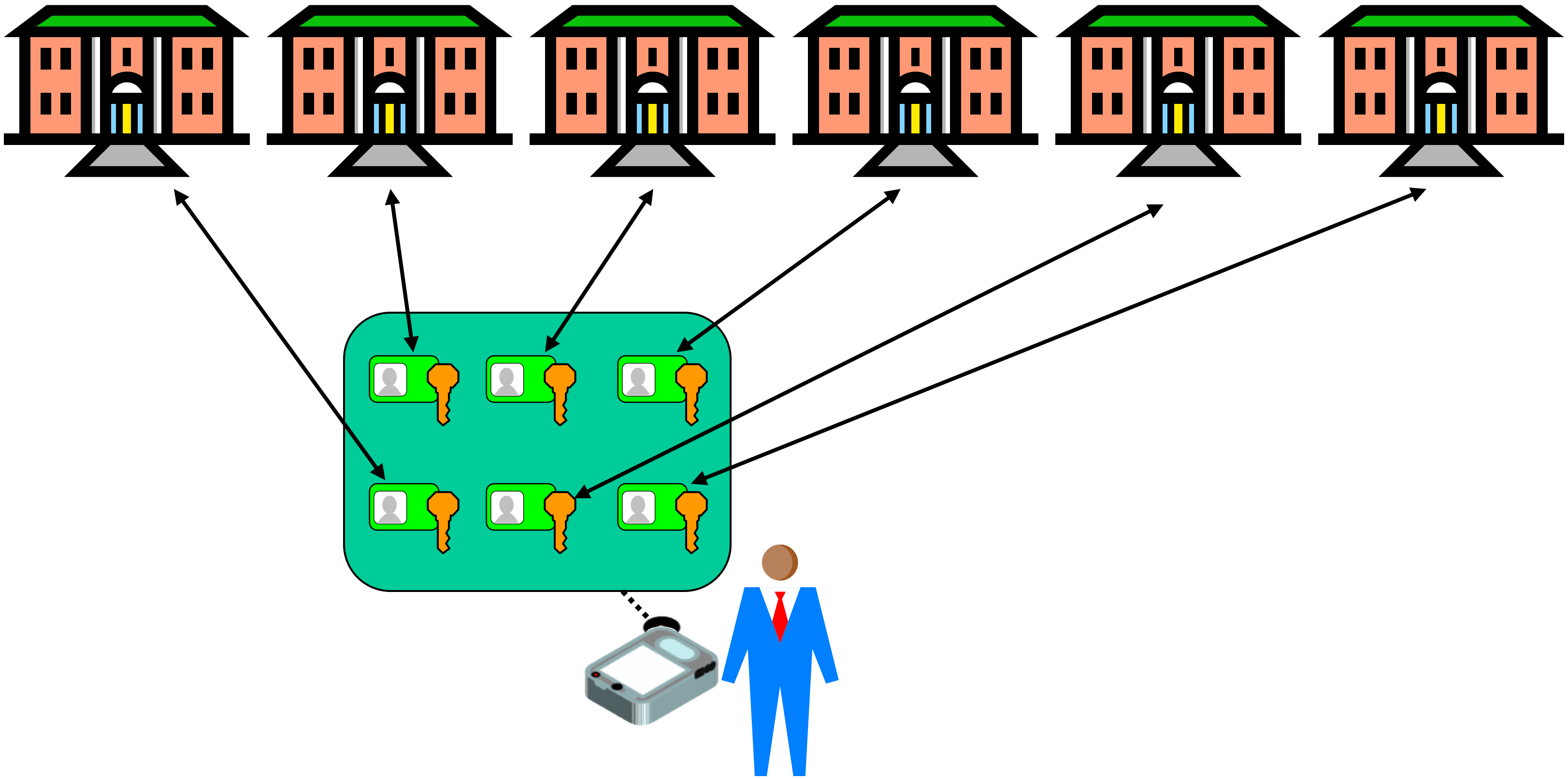


Local user-centric model



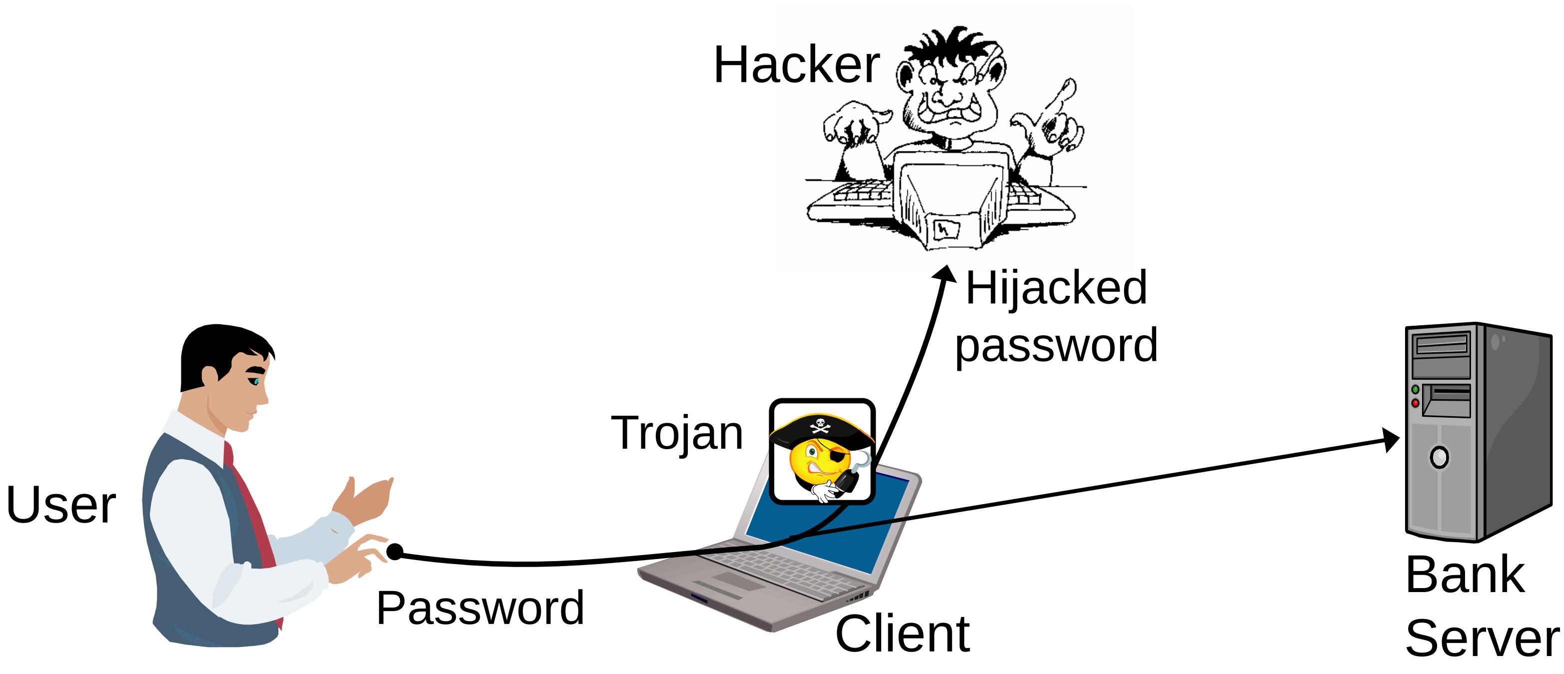
Local user-centric: Imagine you're a customer

Nice and simple



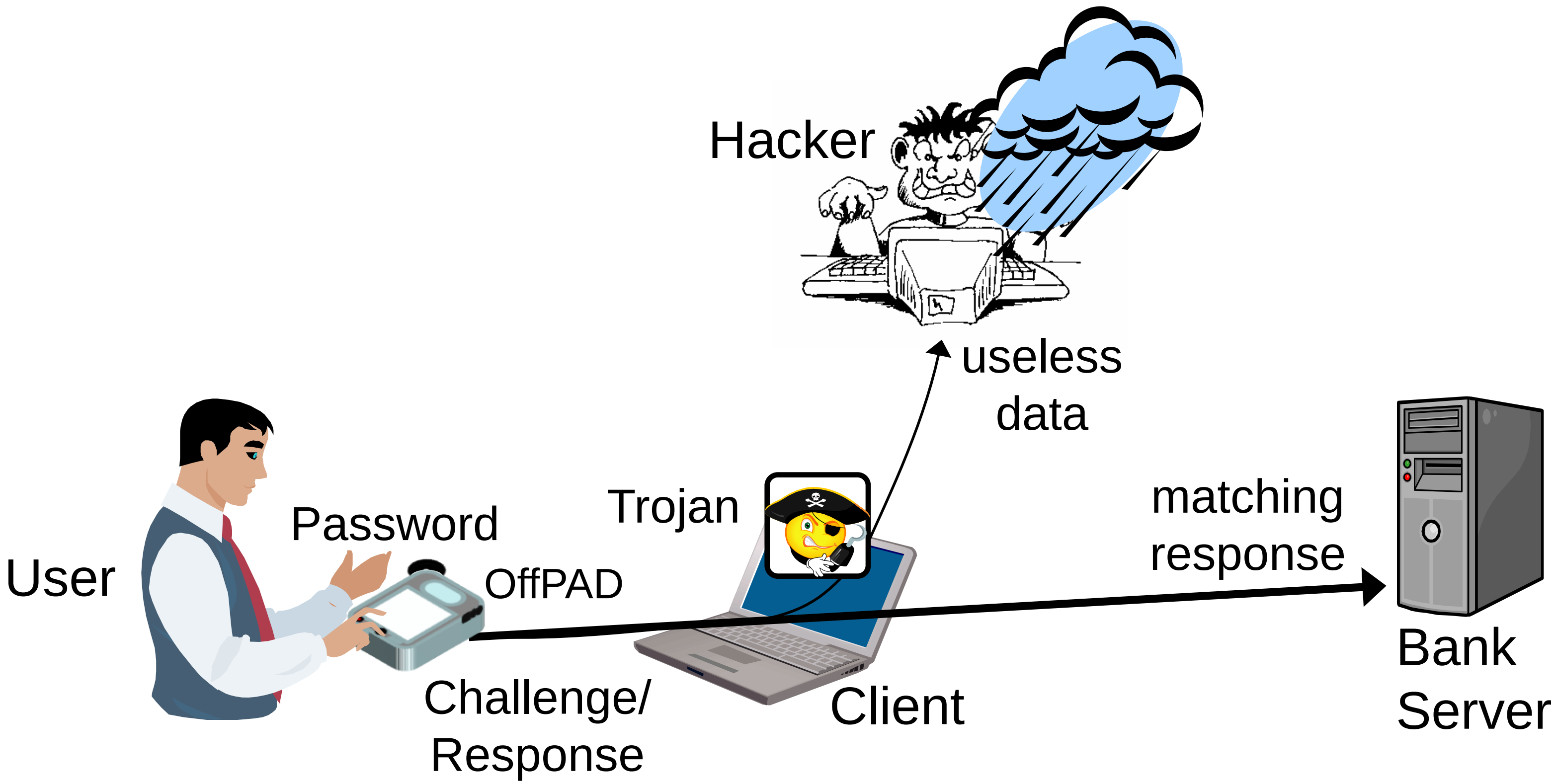
Problem of vulnerable client

- Passwords are typed into client terminal
- Passwords easily get stolen on infected clients



Avoiding password exposure on client

- OffPAD stores passwords
- Only response is exposed to client terminal



OffPAD
Offline Personal Authentication Device

- Limited communication capabilities
- Controlled software
- Integration in authentication protocols