SOITRON

INŠPIRUJEME K NÁROČNOSTI

SPRÁVA ŽIVOTNÍHO CYKLU UŽIVATELE

Roman Pudil, SOITRON

12. 4. 2010

SOITRON

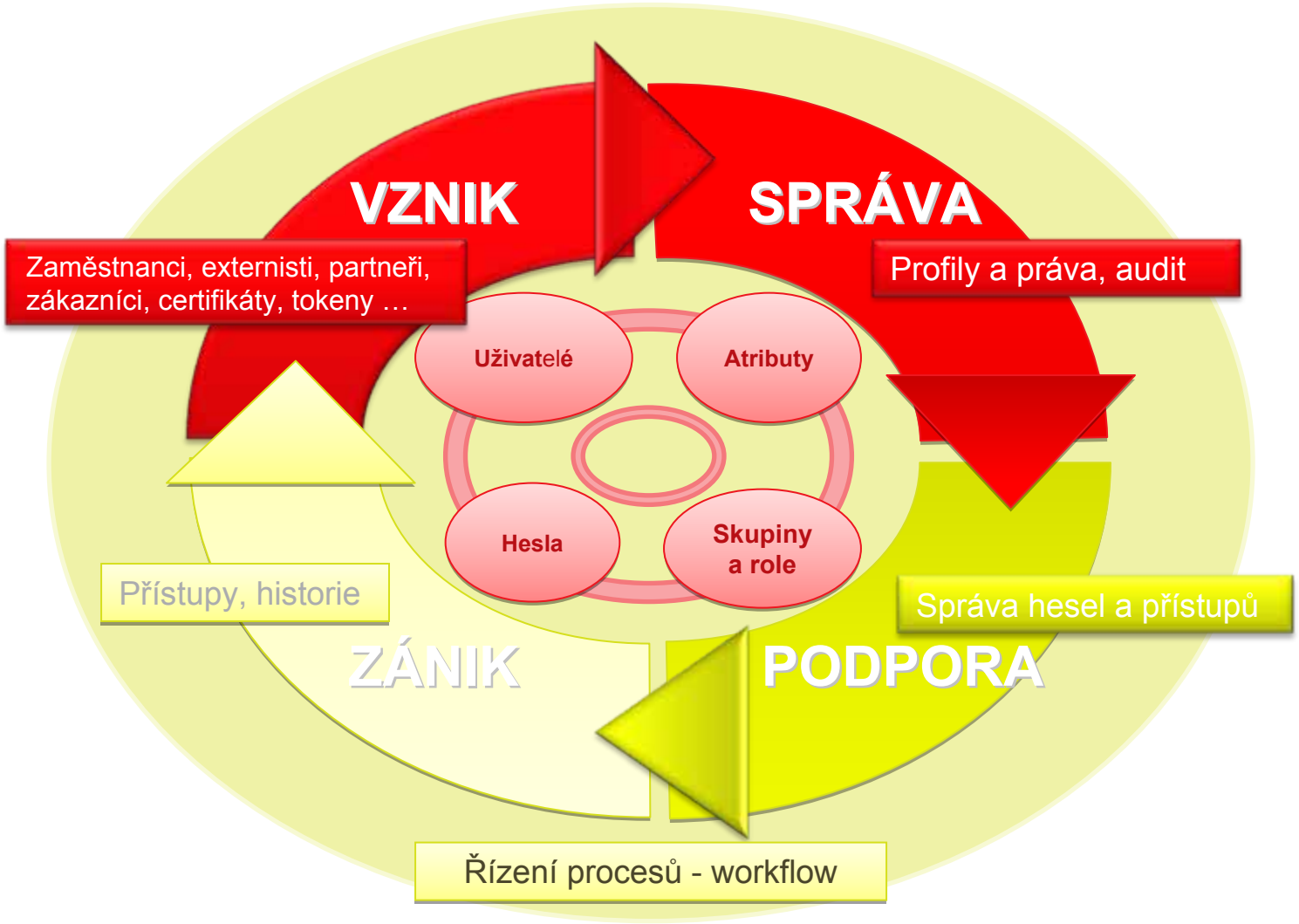
INSPIRUJEME K NÁROČNOSTI

Vymezení pojmů

- Identita = totožnost, shodnost
  - IT identitou může být „cokoliv“ (člověk, místnost, program, …)
- Trezor identit = úložiště dat
  - Systém správy identit zajišťuje bezpečné uložení dat o identitách
- Provisioning = poskytnutí, poskytování, propůjčení
  - Systém správy identit zajišťuje on-line kontrolované a řízené poskytování informací o identitě ostatním systémům v jimi požadované formě nebo její reprezentace v koncových systémech
- Rekonsilace = získání
  - Systém správy identit zajišťuje on-line kontrolované a řízené získávání informací o identitě z autoritativních systémů
- Self Management = samospráva, samoobsluha
  - Může/nemusí souviset s řešením správy identit
- Password Synchronization = synchronizace hesla
  - Může/nemusí souviset s řešením správy identit

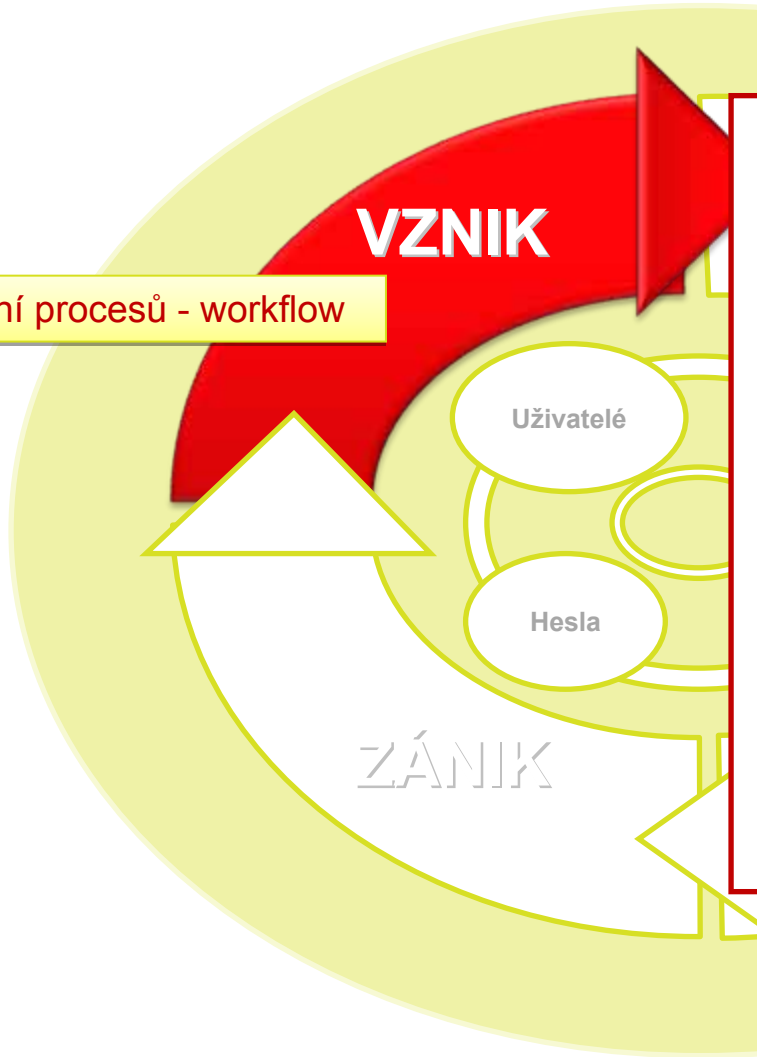
SOITRON
INŠPIRUJEME K NÁROČNOSTI

Životní cyklus identity



SOITRON
INŠPIRUJEME K NÁROČNOSTI

Příchod nového zaměstnance

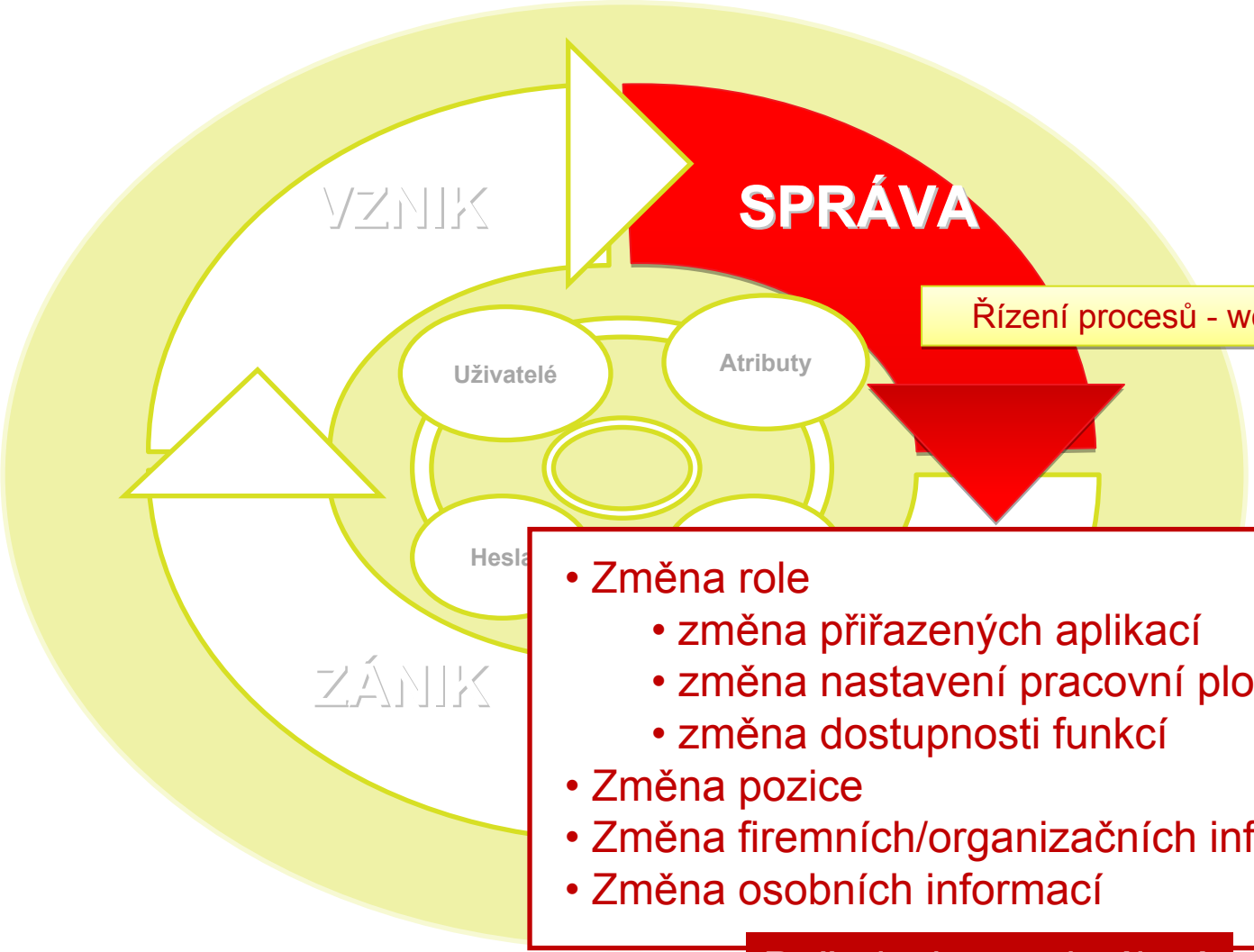


- Jednoznačná identifikace uživatele
- Jednoznačné označení uživatele
  - generování korporátního login name
  - generování emailové adresy
  - generování certifikátů
- Jednoznačné přiřazení účtů identitě
  - generování hesla a jeho propagace a synchronizace
- Jednoznačné určení role
  - přiřazení aplikací
  - uplatnění politik

Požadavky a schválení

SOITRON
INŠPIRUJEME K NÁROČNOSTI

Pozice a vlastnosti se mění...

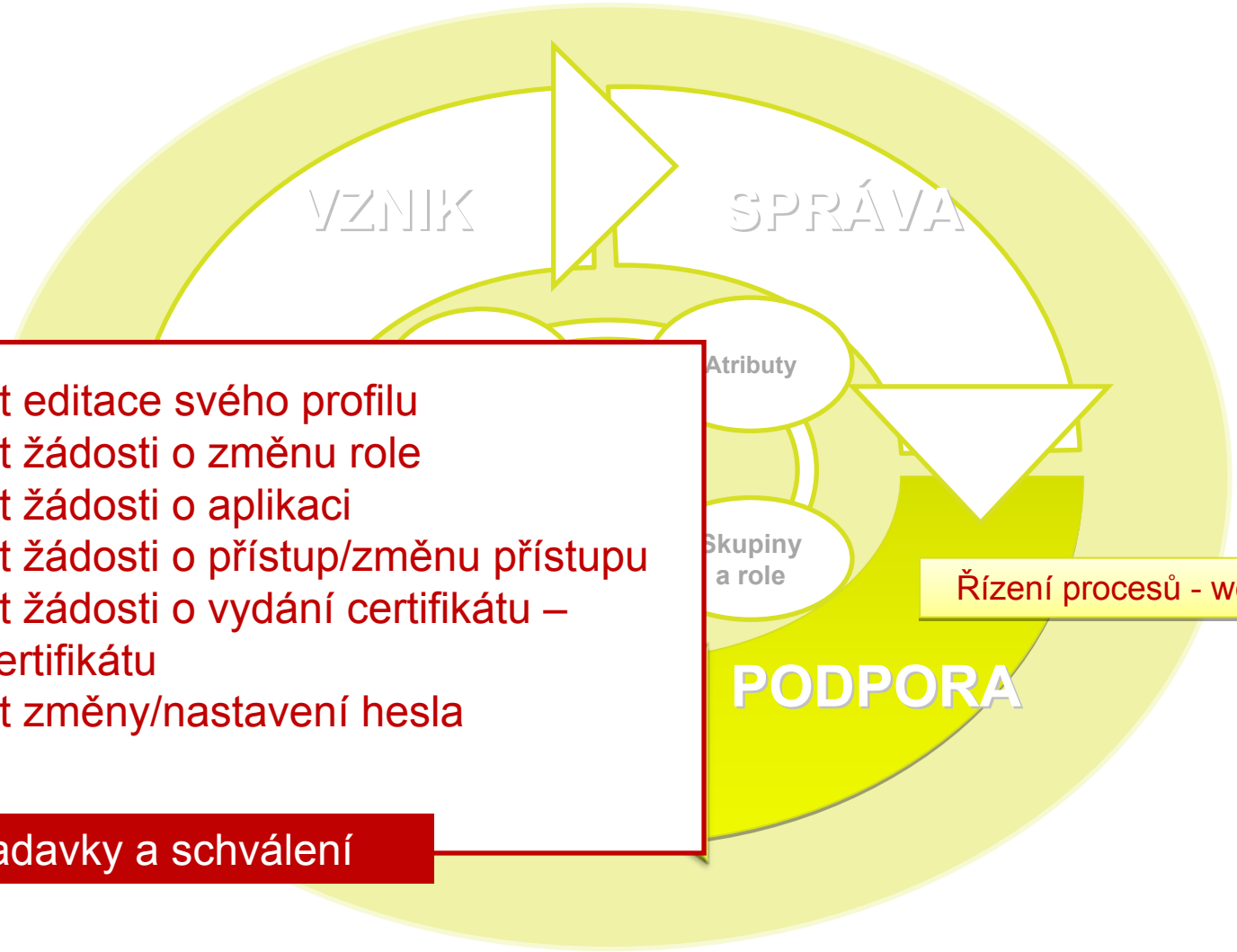


- Změna role
  - změna přiřazených aplikací
  - změna nastavení pracovní plochy
  - změna dostupnosti funkcí
- Změna pozice
- Změna firemních/organizačních informací
- Změna osobních informací

Požadavky a schválení

SOITRON
INŠPIRUJEME K NÁROČNOSTI

Zaměstnanec chce svoje...



- Možnost editace svého profilu
- Možnost žádosti o změnu role
- Možnost žádosti o aplikaci
- Možnost žádosti o přístup/změnu přístupu
- Možnost žádosti o vydání certifikátu – stažení certifikátu
- Možnost změny/nastavení hesla

Požadavky a schválení

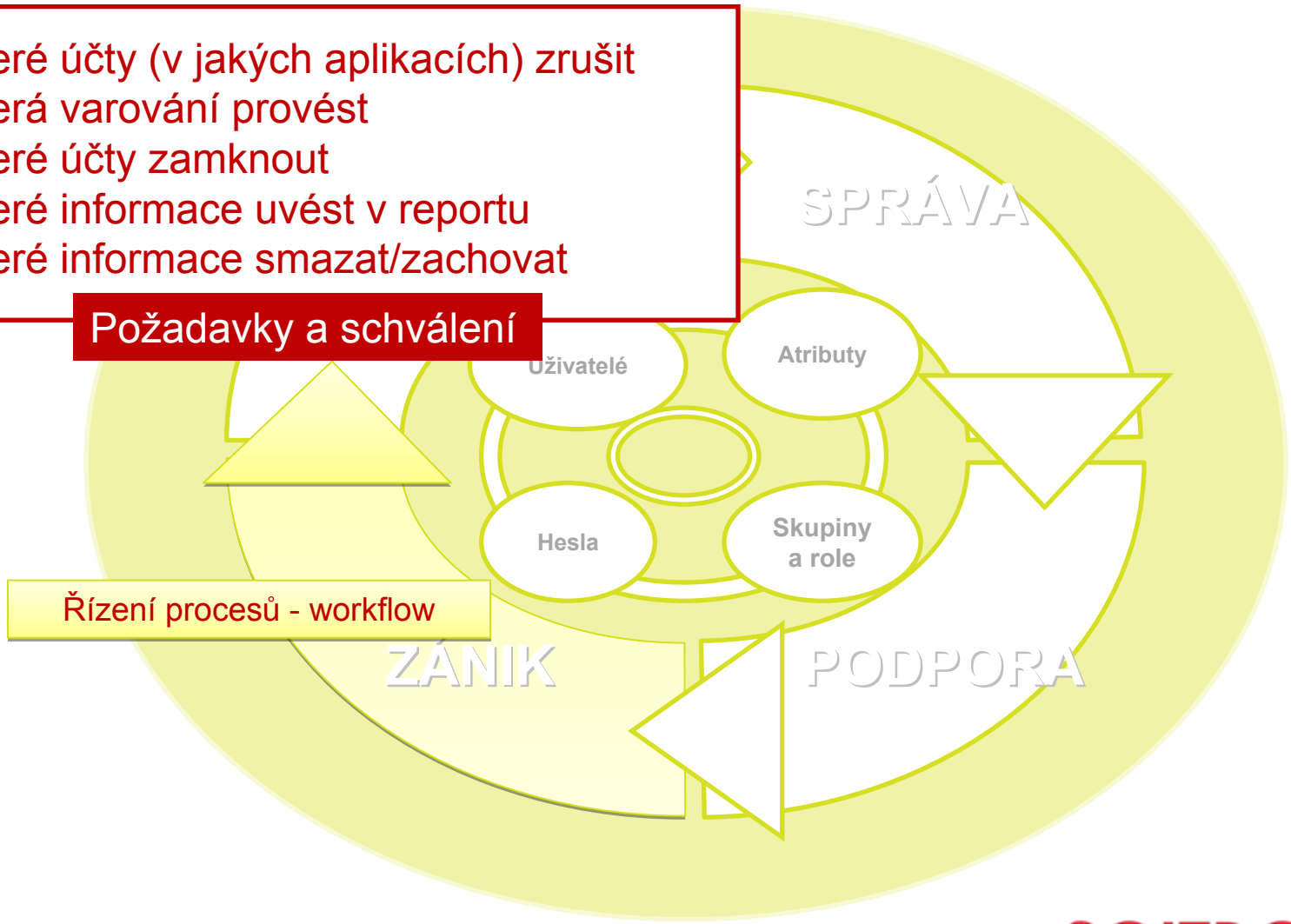
Řízení procesů - workflow

SOITRON
INŠPIRUJEME K NÁROČNOSTI

Odchází, ale nezmizí...

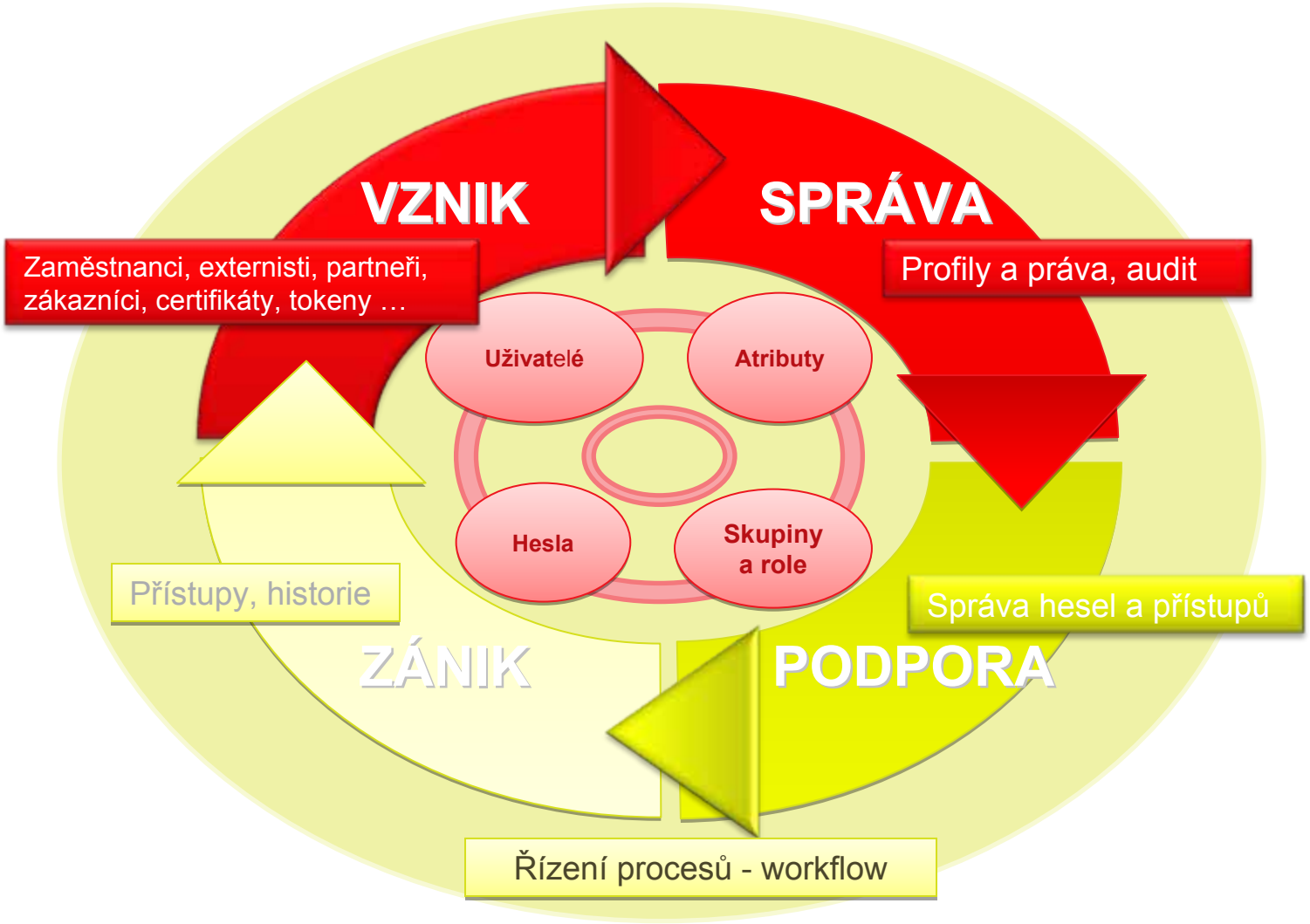
- Které účty (v jakých aplikacích) zrušit
- Která varování provést
- Které účty zamknout
- Které informace uvést v reportu
- Které informace smazat/zachovat

Požadavky a schválení



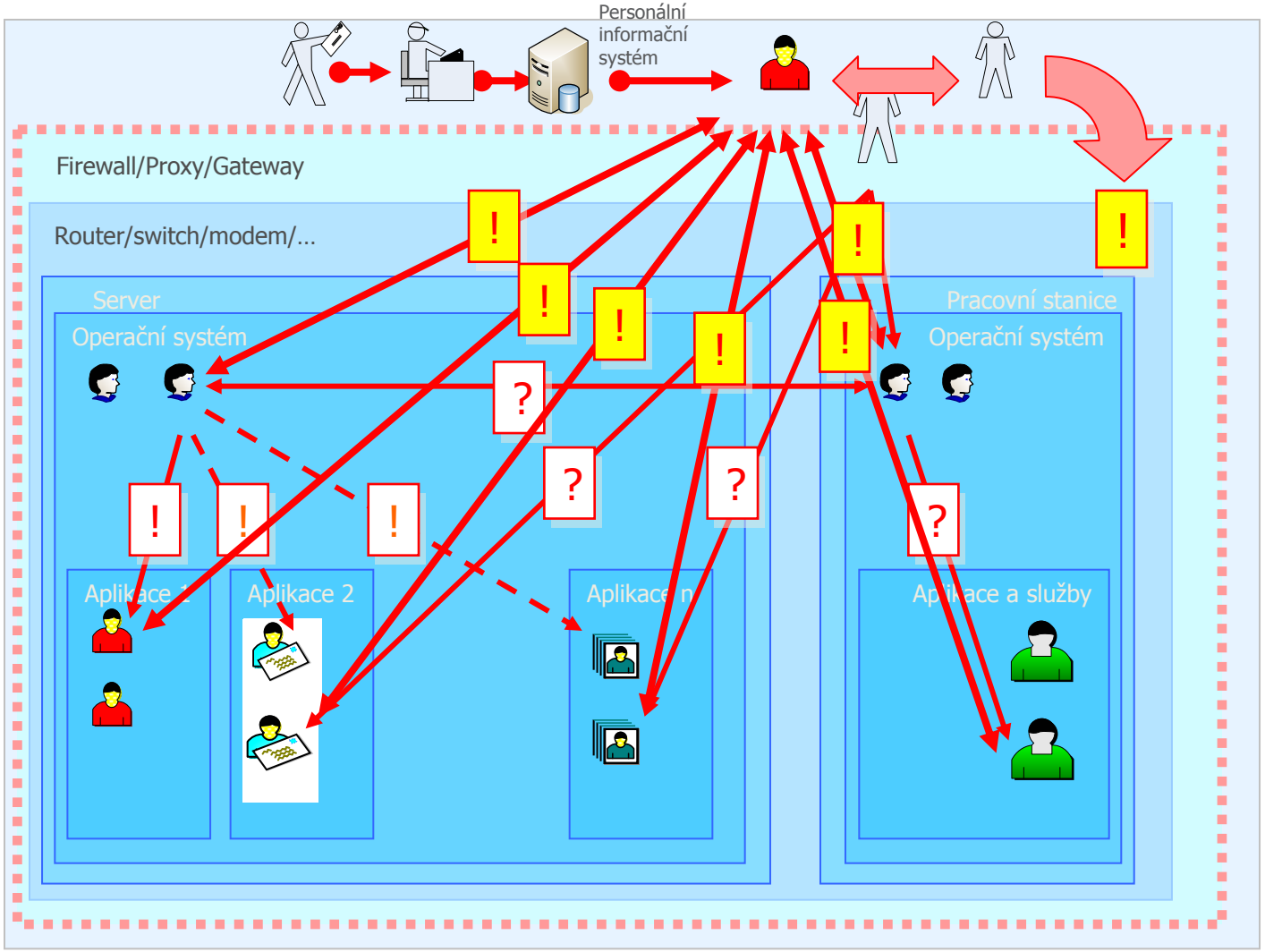
SOITRON
INŠPIRUJEME K NÁROČNOSTI

Tak ještě jednou...



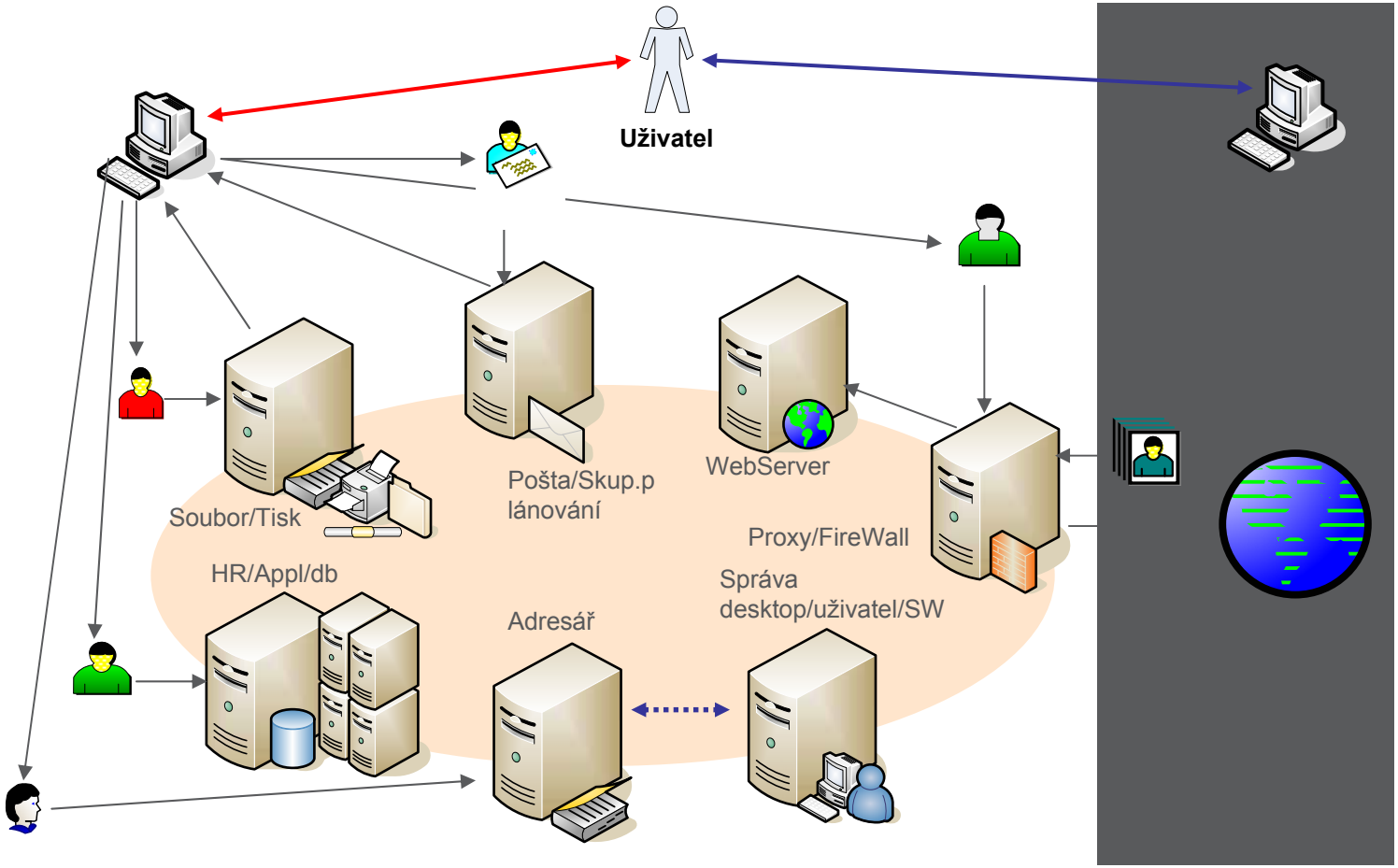
SOITRON
INŠPIRUJEME K NÁROČNOSTI

Bezpečnostní kontext zaměstnance



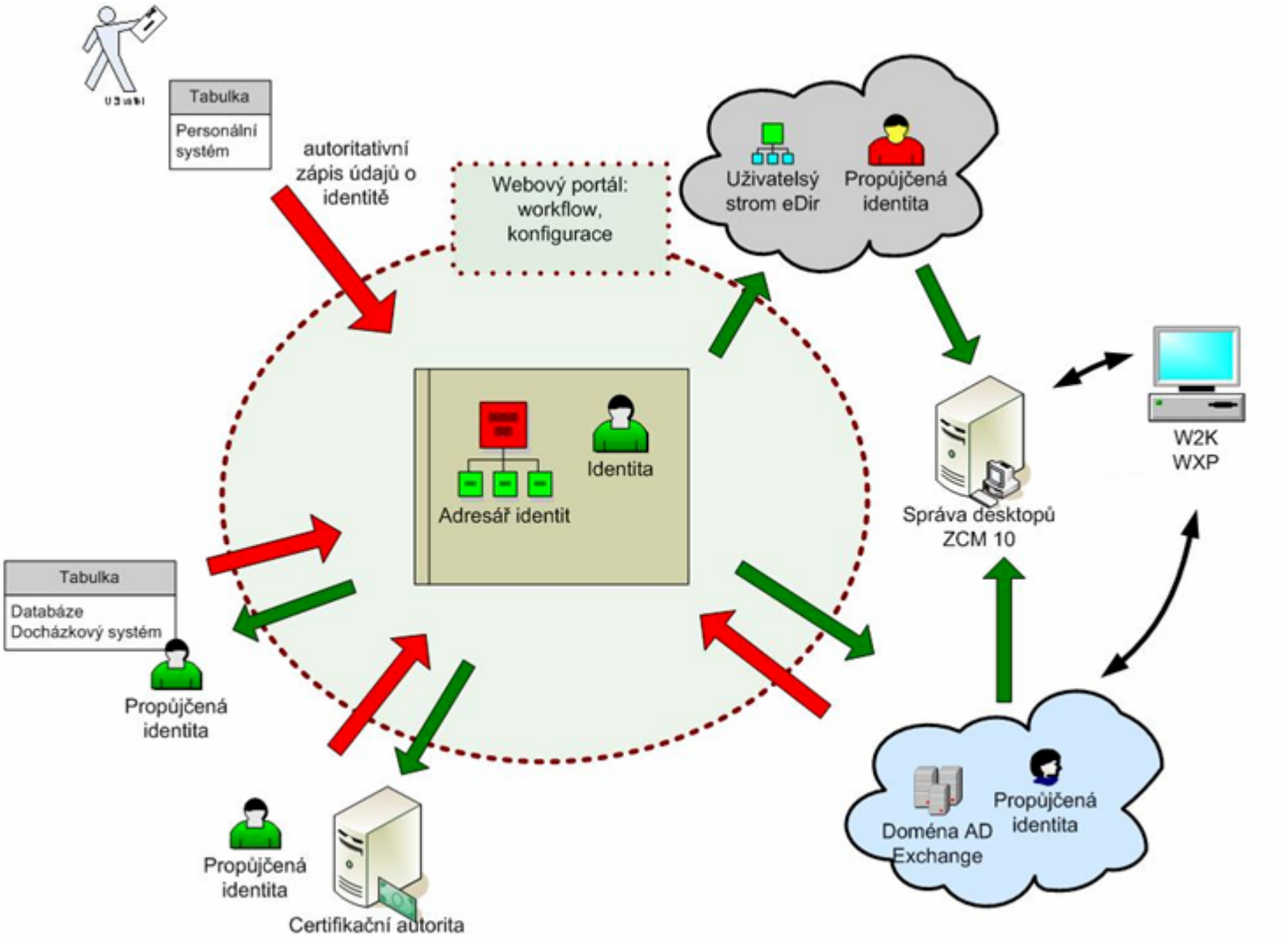
SOITRON
INŠPIRUJEME K NÁROČNOSTI

Stav v organizacích



SOITRON
INŠPIRUJEME K NÁROČNOSTI

Příklad IT systému s implementací IDM



SOITRON
INŠPIRUJEME K NÁROČNOSTI

Komponenty IDM

- **Správa identit (*Management of Identities*)**
  - **Provisioning/deprovisioning účtů**
  - **Automatizace řízení procesů (*Workflow automation*)**
  - **Delegovaná správa (*Delegated administration*)**
  - **Synchronizace hesel (*Password synchronization)***
  - **Samoobsluha (*Self Service*)**
- **Řízení přístupu (*Access Control*)**
  - **Správa přístupů (*Access Management*) zahrnuje správu dat o**
    - **identitě uživatele**
    - **autentikaci uživatele**
  - **Řízení přístupu pomocí politik (*Policy based access control*)**
  - **Přístup jediným přihlášením (*Enterprise/Legacy Single Sign On - SSO and Single Signout)***
  - **Přístup k web aplikacím jediným přihlášením (*Web Single Sign On*)**

SOITRON

INŠPIRUJEME K NÁROČNOSTI

Komponenty IDM

- **Adresářové služby (*Directory Services*)**
  - **Bezpečné úložiště identit - správu účtů a jejich atributů**
  - **Replikace/synchronizace**
  - **LDAP, X.500**
  - **IBM/Tivoli, Microsoft, Novell, Oracle ID, Sun/iPlanet**
- **Jiné související kategorie**
  - **Audit (kdo-kam-kdy-jako kdo- …)**
  - **Řízení přístupů na základě rolí (*Role-based Access Control*)**
  - **Řízení přístupů na základě pravidel (*Rule-based Access Control*)**
  - **Federace přístupů**

DĚKUJI

Roman.Pudil@soitron.com

SOITRON
INŠPIRUJEME K NÁROČNOSTI