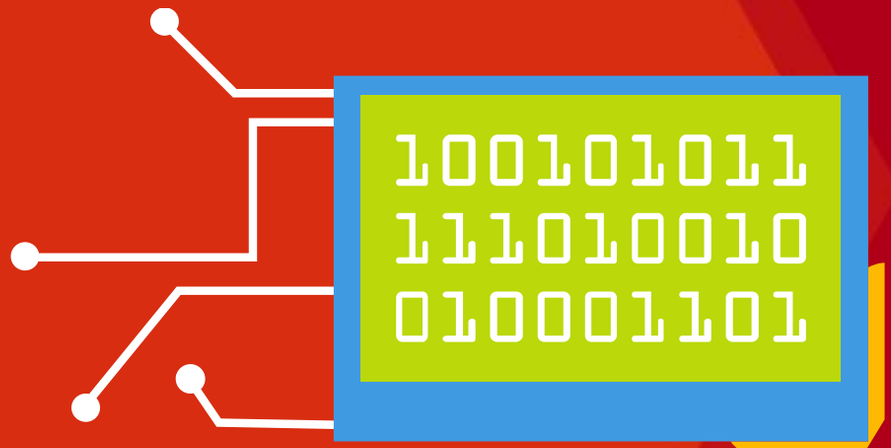
KONFERENCA

Microsoft

Upravljanje Identitete
Kaj je že to?



Elvis Guštin, MVP

EM-Soft sistemi d.o.o.

TEHNOLOGIJA

Zakaj ravno ID management?

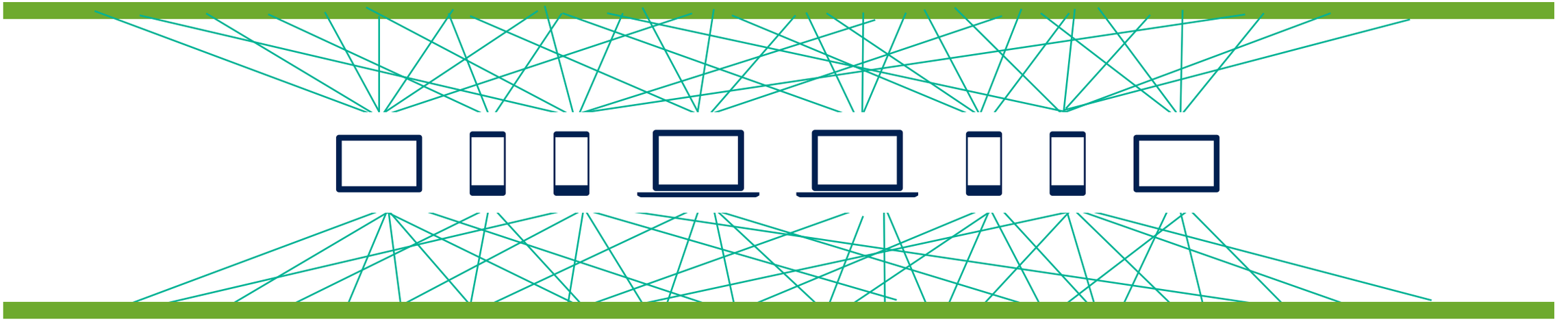
- Avtentikacija / Avtorizacija se spreminja
  - Acitve Directory (leto 2000…)
  - Spletni servisi
  - Cloud in spletne aplikacije
- Naše okolje se ne konča več pri „Firewallu“ ampak je brez končnih točk
- IT služba ne more več nositi odločitev za podeljevanja vseh dovoljenj
- Uporabniki imajo vedno več problemov z login podatki (Single Sign On)
- Microsoftove besede (tehnična konferenca – Amsterdam 2017)
  - Identity is the new surface of attack
  - Identity is the new security parameter

KONFERENCA

Trenutno stanje v večini podjetij

HIGHTAIL Dropbox amazon web services™ Microsoft Azure EC2 Microsoft Dynamics box CONCUR Basecamp®

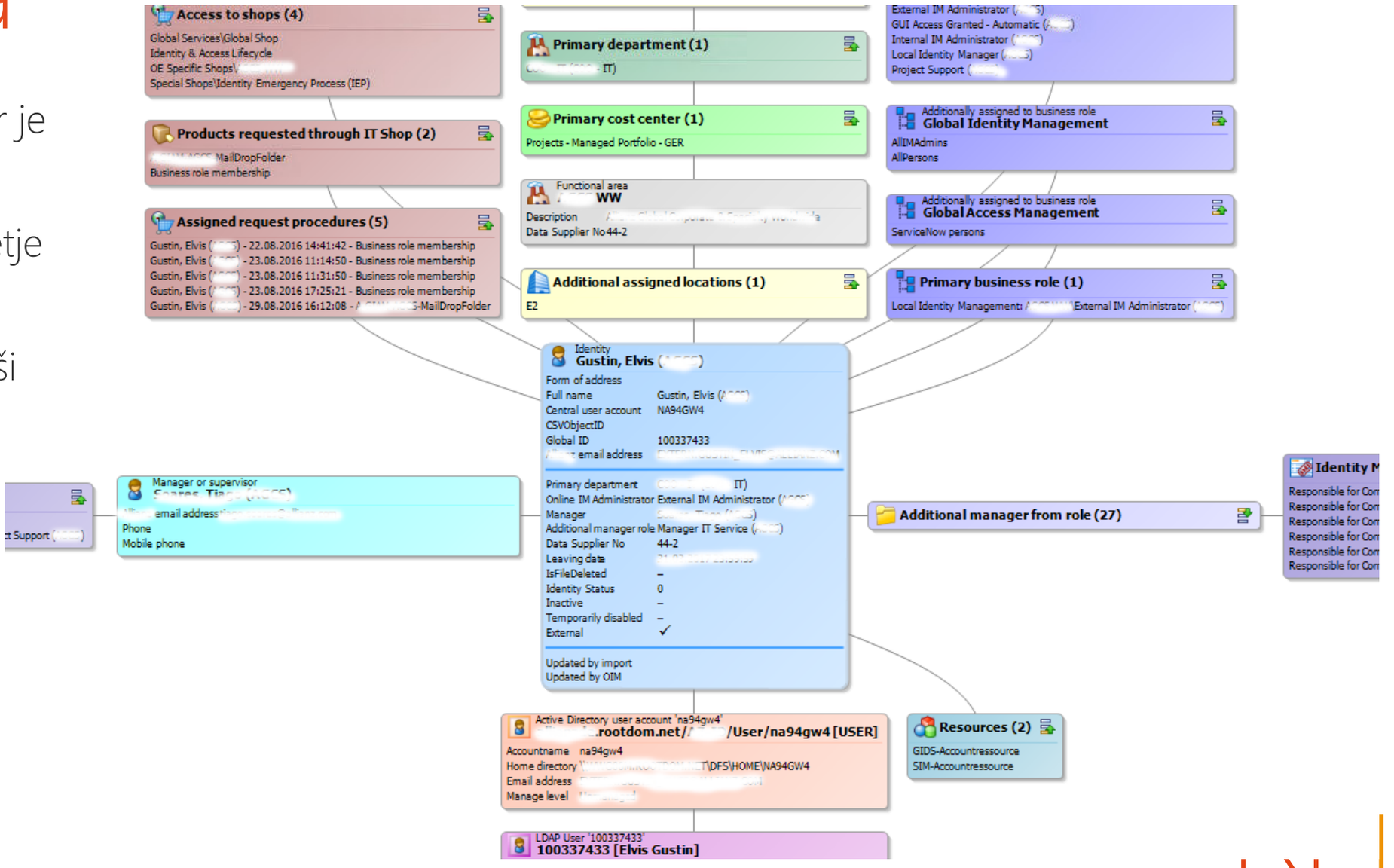
ShareFile by CITRIX GoToMeeting by CITRIX salesforce.com force.com Office 365 SAP SUGARCRM Microsoft System Center



On-premises	Managed devices	Active Directory
		Windows Server

Groza ID-ja

- Samo Print screen – ker je cela slika prehuda
- Mislite da je vaše podjetje drugačno?
- Veste do česa imajo vaši uporabniki dostope?
- Veste kaj narediti pri premikih, odpovedih,…



KONFERENCA

Struktura organizacije

- Vsako organizacijo moramo najprej opredeliti
- Strukture vedno postanejo večtirne – ni možnosti enoličnega določanja
  - Razdelitev po fizičnih lokacijah
  - Razdelitev po oddelkih
  - Razdelitev po Cost centrih (uporabljajte raje Profit centre)
- Te razdelitve se med seboj ne popolnoma prekrivajo – morajo biti neodvisne
  - Oddelek je lahko na več lokacijah
  - Profit center ima lahko v sebi več oddelkov (in samo delno)
- Zaposleni se lahko znajde v eni ali več delih strukture – stalno ali le za določen čas (projekt, poslovne vloge)

KONFERENCA

Identitete (računi)

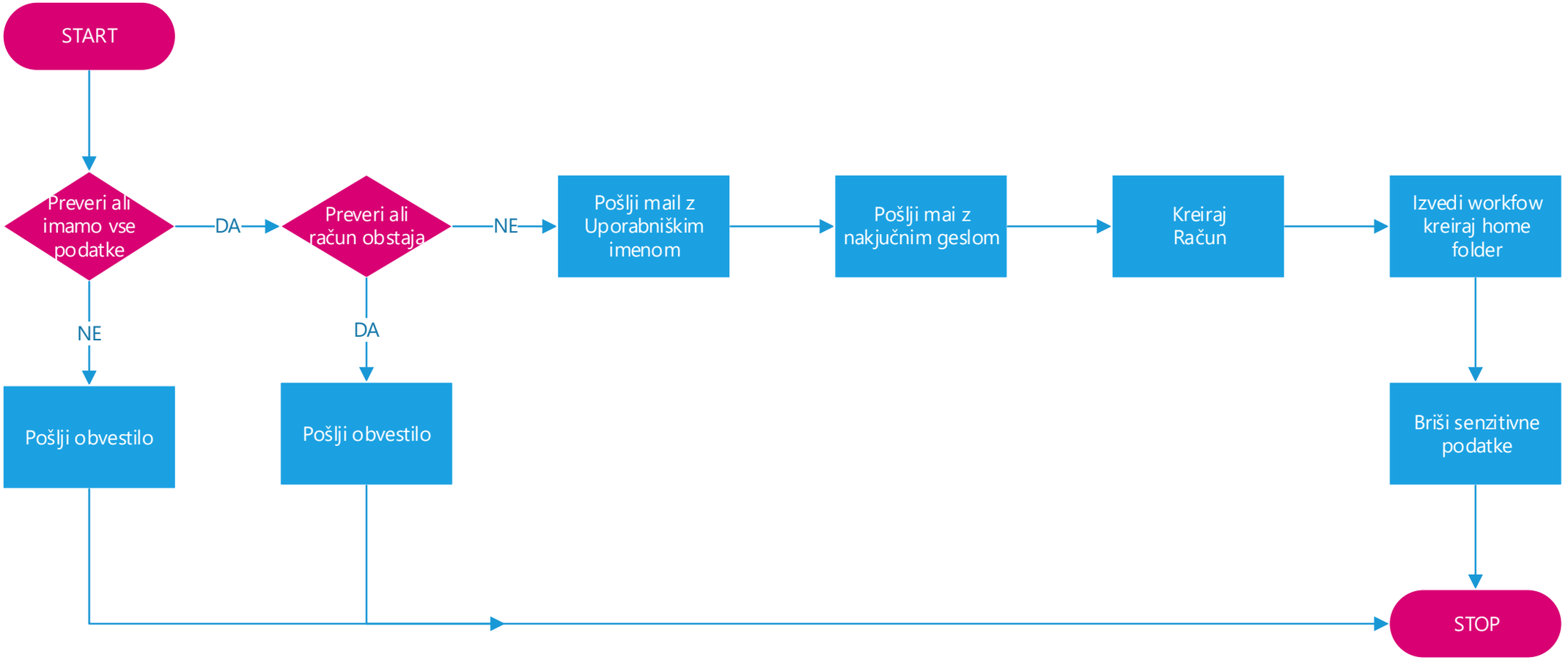
- Govorimo o IDENTITETAH, no o računih, pravicah in dostopih
- Ni več „glavnega mehanizma“ (npr. AD)
- Ustvarjanje in onemogočanje (brisanje???) identitet mora biti samodejno
- Pojavi se nam veliko različnih sistemov
  - Med seboj so enakovredni
  - Uporabnik mora biti „Unique“ po celotni platformi
  - Razmišljati moramo tudi na različne načine prijave (username, mail, ….)
- Vsako spreminjanje / kreiranje mora imeti svoj workflow - potrjevanje

Kako mora ID management delovati

- Celoten proces mora temeljiti na Workflow engine-u:
  - Assignment (of anything)
    - To so lahko računi, članstvo v grupah, globina dostopa do aplikacije, lokacije, helpdesk center,…
  - Removing (of anything)
    - Kar dodelimo moramo tudi odvzeti. Pazite na sledljivost (zakaj bi brisal?)
  - Periodično preverjanje in security index
    - Sistem je edini v podjetju, ki ima nadzor nad vsemi dostopi uporabnika
    - Edini lahko izračuna (preveri) ustreznost in rizičnost kombinacije dostopov – *separation of duty*
    - Periodično pošiljajte potrjevanja dostopov odgovornim (udeležba v projektih)
  - Company (global) policy
    - Kot GPO – obvezni tokovi, ki se jih ne da preskočiti
    - Za določene funkcije MORA to nekdo potrditi ali se mora še nekaj zgoditi

KONFERENCA

Workflow: Kreiranje AD računa



KONFERENCA

Auditing – Revizijske sledi

- Tu se stvari kompliciraju zaradi kompleksnosti objektov
- Paziti moramo na veliko faktorjev – postopki in rezultati
- Beležite več različnih vrednosti – podatkov:
  - Atributi – zelo pomembno je, da veste iz česa in v kaj se je spremenil atribut
  - Workflow – pomemben del auditinga, ker pove:
    - Kdo je naročil in potrdil spremembo
    - Zakaj je bila sprememba narejena (udeležba na projektu, sprememba delovnega mesta,…)
  - Konfiguracije
    - Sprememba konfiguracije lahko vpliva na celotne dostope po podjetju (vidni samo kot „samodejno“)
    - Vedeti morate natančno kdo in kdaj je spremembo naredil in kaj sprememba prinaša

Ostale dobre prakse

- Pazite na podporo regionalnim posebnostim
  - Tu niso samo posebni znaki, ampak še veliko več – tudi navade
  - Različne vrste imen (Indija – local name + global name)
  - Jezik včasih pomeni več, kot si mislite
  - Zaradi lokalnih zakonov imamo lahko včasih zelo veliko problemov (podatki)
  - HR programi – isto podjetje ima lahko več različnih lokalnih programov
- Pazite na možnost povezave z zunanjimi aplikacijami
  - Active Directory, Exchange in SharePoint so tu zgolj en sistem – ne glavni
  - SAP, Pantheon, Service Now, Sales Force in druge nestandardne aplikacije lahko zahtevajo znanje za izdelavo konektorjev.
  - Pazite na različna delovanja avtentikacij in globino integracije
  - Verjetno 100% avtentikacij ne boste pokrili (E-Davki)

KONFERENCA

In še nekaj malenkosti

- Poizkusite narediti Self service portal – web vmesnik za:
  - Kreiranje novih zahtevkov (dostop do aplikacij, sistemov, funkcij,…)
  - Razna preverjanja (kaj imajo podrejeni) in poročila
  - Pazite na osebne podatke in lokalizacijo (jezik je pomemben)
- Naredite pametna poročila in obveščanja
  - Veliko obveščanj ima isti rezultat, kot ostala spam pošta
  - Poročila morate redno generirati in spremljati (dodeljeni dostopi, porabljene licence, …)
  - Ne pozabiti na obvestila potrditev zahtevkov – po možnosti imejte rezervni scenarij (dopust odgovornega)
  - Posebno pozornost namenite obvestilom pred ukinitvami dostopov
  - Uporabljajte standardne forme, izraze in enote

KONFERENCA

Kdo naj sodeluje pri projektu – pot identitete

- Za uspešen projekt rabimo sponzorja v vodstvu in HR. Sodelujejo pa tudi službe za strukturiranje organizacije, security, pravna služba, IT,…
- 90% časa se boste samo dogovarjali in risali po papirju
- Uporabljajte načelo „Less is more“ – ne kompliciraj s funkcijami
- Identiteta se mora držati poti osebe:
  - Prične se z zaposlitvijo v kadrovski službi
  - Nadaljuje skozi dodeljevanje osnovnih – standardnih obvez
  - Lahko povprašuje po nestandardnih pravicah
  - Konča se v kadrovski službi
- Ne pozabite, da se identiteta v času lahko spreminja
  - Prezaposlitev na drugo mesto (podjetje)
  - Zamenjava osebnih podatkov (priimek)

KONFERENCA

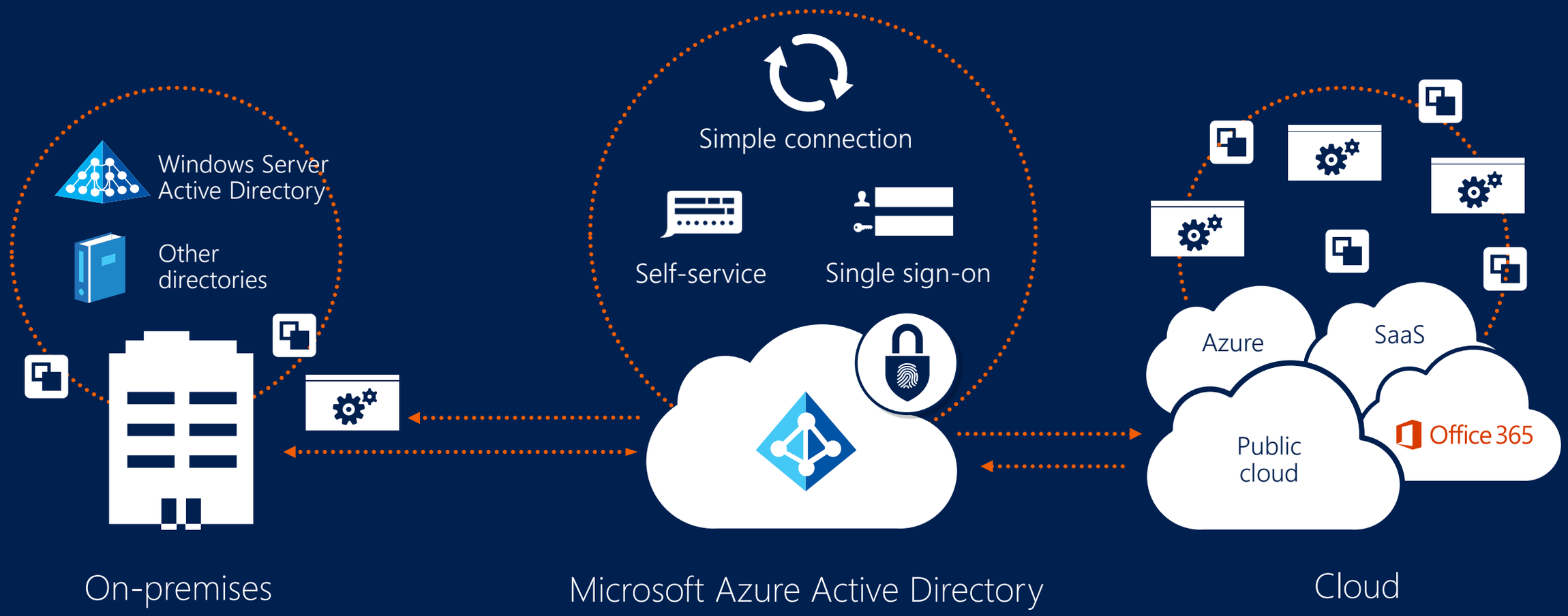
Microsoft in ID management

- Včasih je bil FIM
  - Dober produkt za svoj čas, precej kompliciran vpeljava
- Zgodba s Cloudom (Azure Active Directory)
  - Zelo dober način prijema, katerega uporabo priporočam
  - Dobro narejen SSO, že podpira veliko aplikacij
  - Ogromne možnosti nadzora v Cloud-u Azure in O365 integracija
  - Integracija z lokalnim AD in možnost dinamičnih skupin
  - Ni celoten produkt – se ne začne in konča v HR pisarni
- Microsoft MIM
  - Naslednik FIM-a
  - Skupaj z AAD-jem tvori celoto
- V prihodnosti bo samo AAD – funkcionalno bo pokrival tudi MIM

KONFERENCA

Ne pozabite: AAD je trenutno le del zgodbe

- AAD ne vsebuje zajema začetnih podatkov, je večinoma avtentikacijski mehanizem



MIM vs. Azure Active Directory

	Azure Active Directory	Microsoft Identity Manager
Password reset/management	YES	YES
Group management	YES, not dynamic	YES
Provisioning, deprovisioning	NO	YES
Certificate management	NO	YES
Role-based access control	NO	YES

Microsoft Identity Manager 2016 features

Cloud-ready identities

- Standardized Active Directory attributes and values
- Partitioned identities for synchronization to the cloud
- Easier-to-deploy reporting connected to Azure Active Directory
- Preparation of user profiles for Microsoft Office 365

Powerful user self-service

- Self-service password reset with Multi-Factor Authentication
- New REST-based APIs for AuthN/AuthZ
- Self-service account unlock
- Certificate management support for multi-forest and modern apps

Enhanced security

- Privileged user and account discovery
- New Windows PowerShell support and REST-based API
- Workflow management: elevated just-in-time administrator access
- Reporting and auditing specific to privileged access management

Vprašanja

Elvis Guštin

elvis@em-soft.si

KONFERENCA