



Op naar IAM 3.0

ISACA round table

drs. André Koot RE CISA CISM
3 juni 2015



AGENDA

- Wie ben ik
- Wat is I A M
- Ontwikkeling IAM
- - RBAC, Federatie
- - ABAC, mobile
- Project



Mijn identiteit

- Specialist Informatiebeveiliging
- Hobby IAM
- @meneer
- Nieuw: Podmin van diaspora* pod.readme.is

Strict

- Onafhankelijk ICT adviesbureau
- Security diensten
 - IB Volwassenheidsbepaling
 - Cybersecurity Scan
 - Cloudsecurity
 - Security architectuur
 - Identity & Access Management

Wie mag wat en waarom is dat zo?

- Wie
 - Identiteitenbeheer
- Wat
 - Autorisatiemanagement
- Waarom
 - Access Governance...!

Aanmaken



Verwijderen

Bijwerken

Wie mag wat en waarom is dat zo?

- Autorisatiebeheer
 - Bepalen autorisaties
 - Definiëren autorisaties en combinaties
 - Rollen...
 - Modelleren autorisatiemodellen en -matrices
 - Toekennen en intrekken

Wie mag wat en waarom is dat zo?

- Wie bepaalt dat?
- De eigenaar.
- Hoe doet de eigenaar dat?
- Traditioneel:
 - De eigenaar verstrekt de toegang, de sleutel
 - Ooit gebeurde dat voor elk systeem afzonderlijk
 - Accounts, accounts, accounts etc...

Gebruiks Overeenkomst

Resource owner

Process owner

Process owner

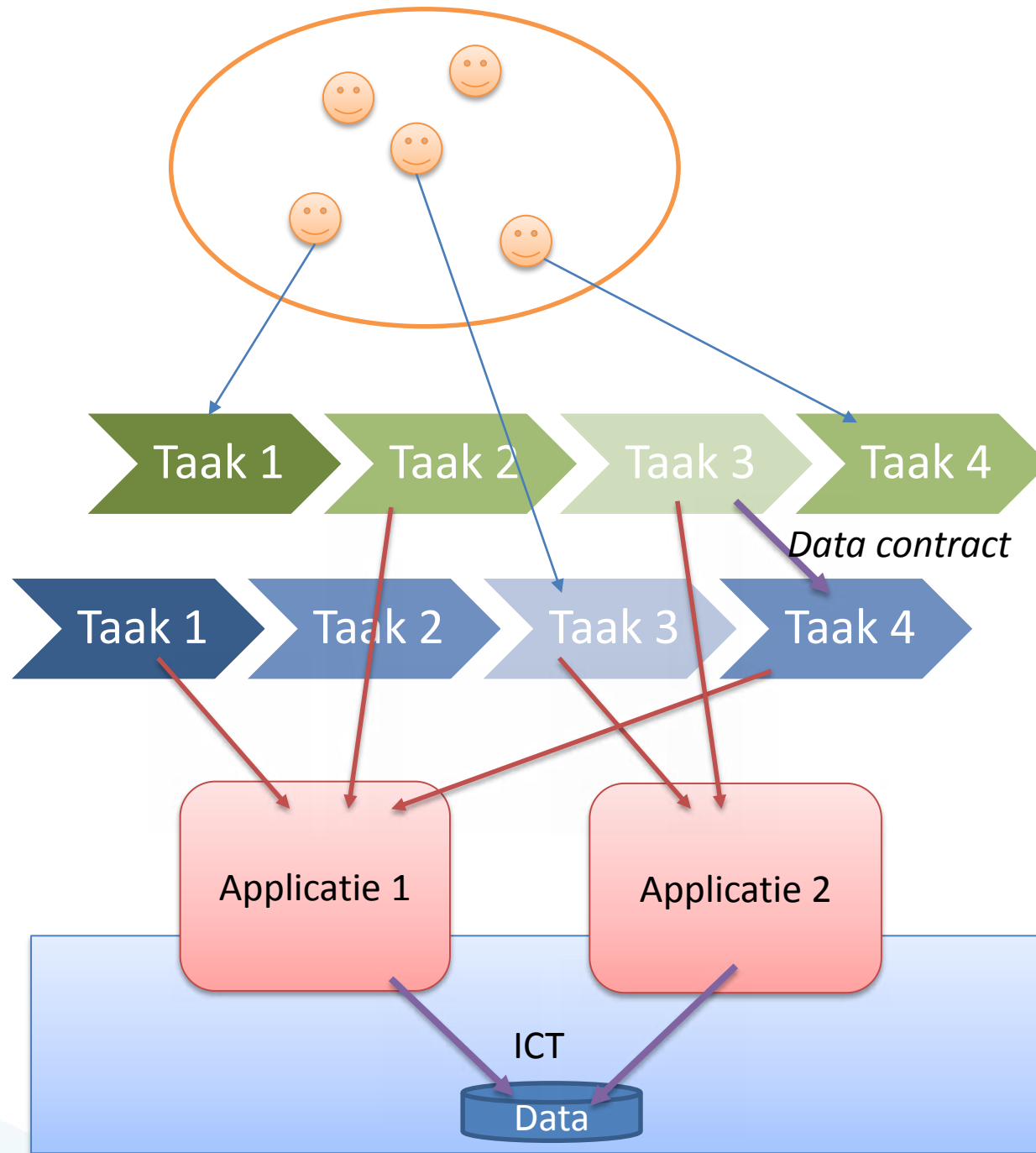
OLA

System owner
(business)

SLA

ICT owner

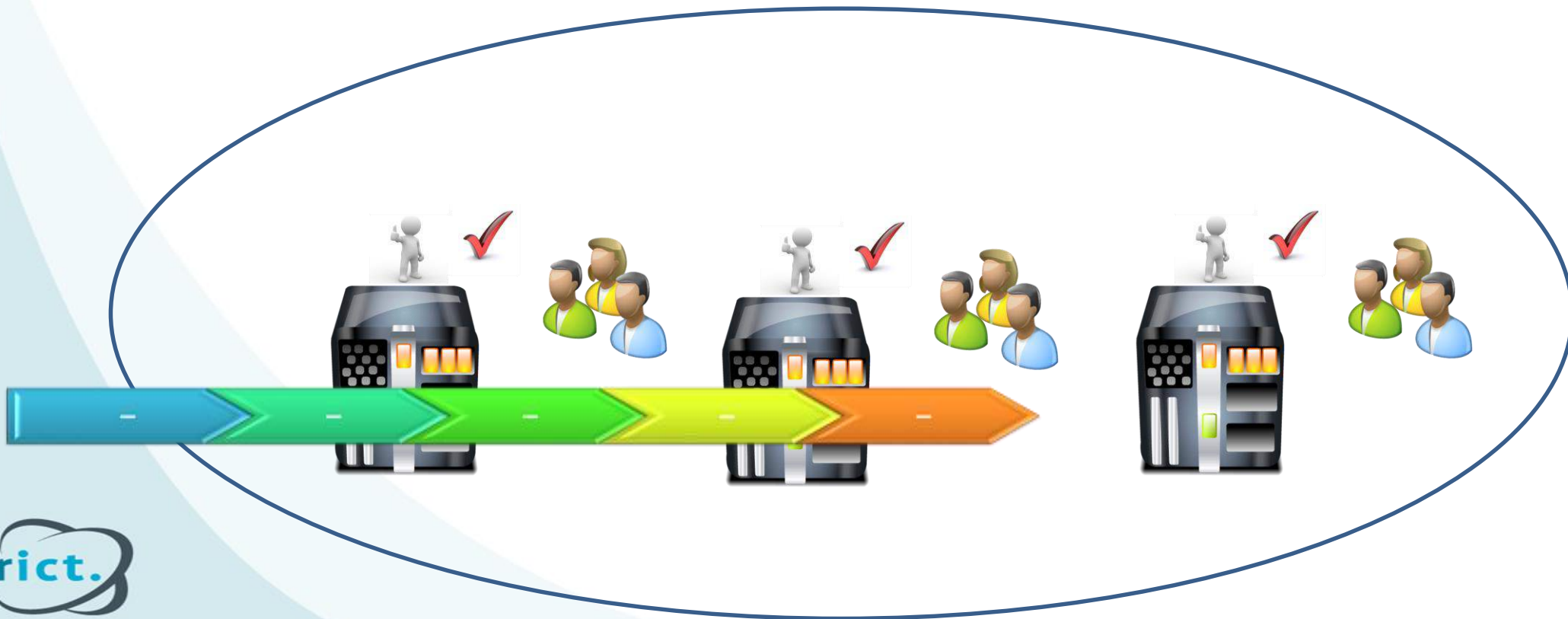
Data owner



- Eigenaar beheert zelf



- Organisatie beheert zelf

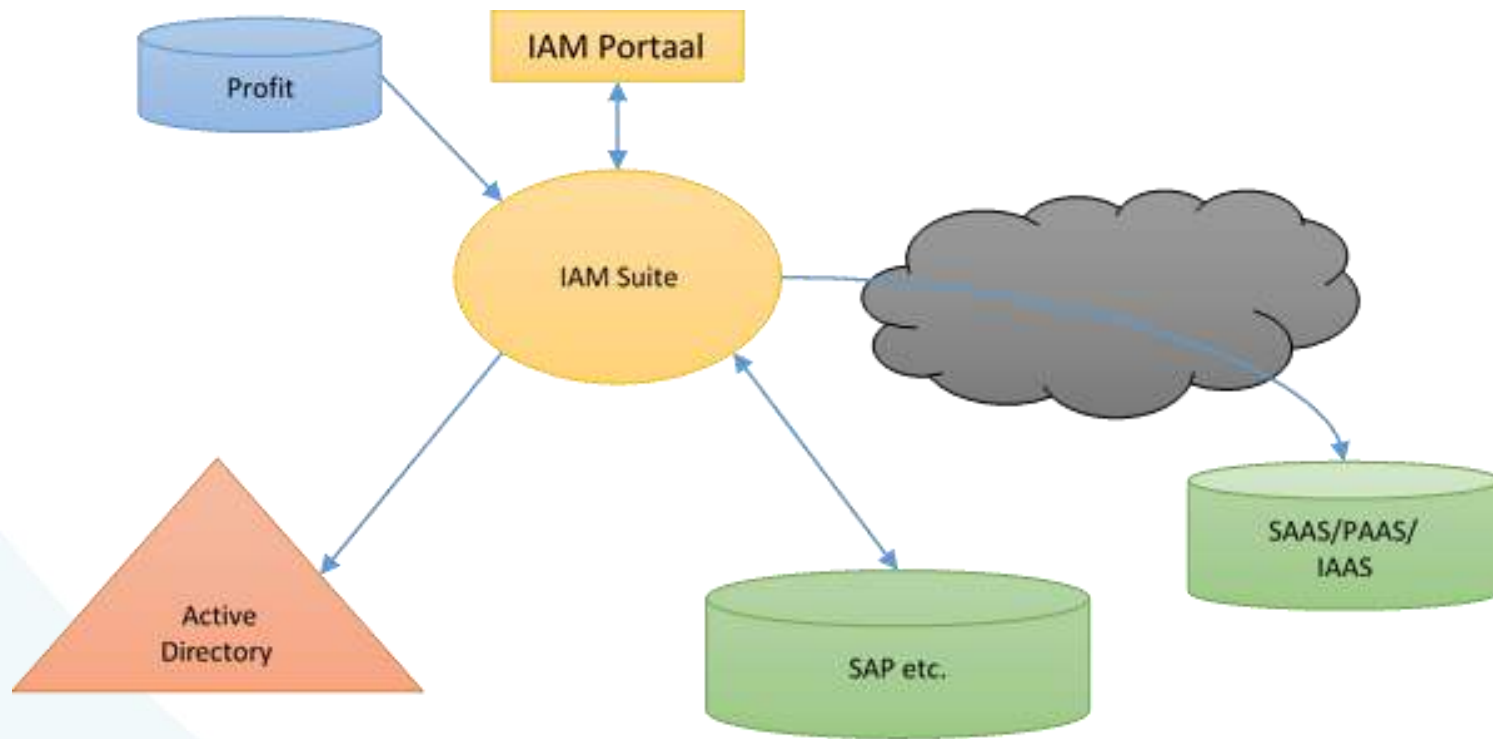


IAM 1.0

- Organisatie beheert zelf



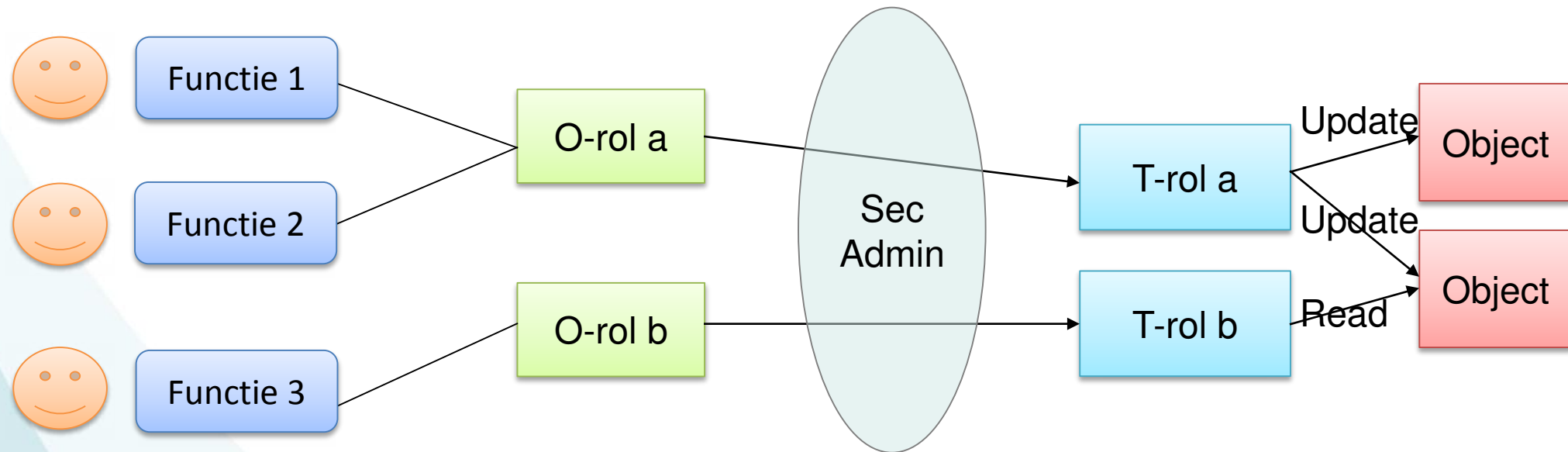
Architectuur



Role Based Access control

- Eenvoud van beheer
- Vereist governance
 - Lijnmanager <> Proceseigenaar <> Systeemeigenaar <> Gegevens eigenaar
 - Functiescheiding en conflicterende rollen
 - Auditors snappen het niet altijd
- Eindig
 - Niet Cloud compatible

Role based access control

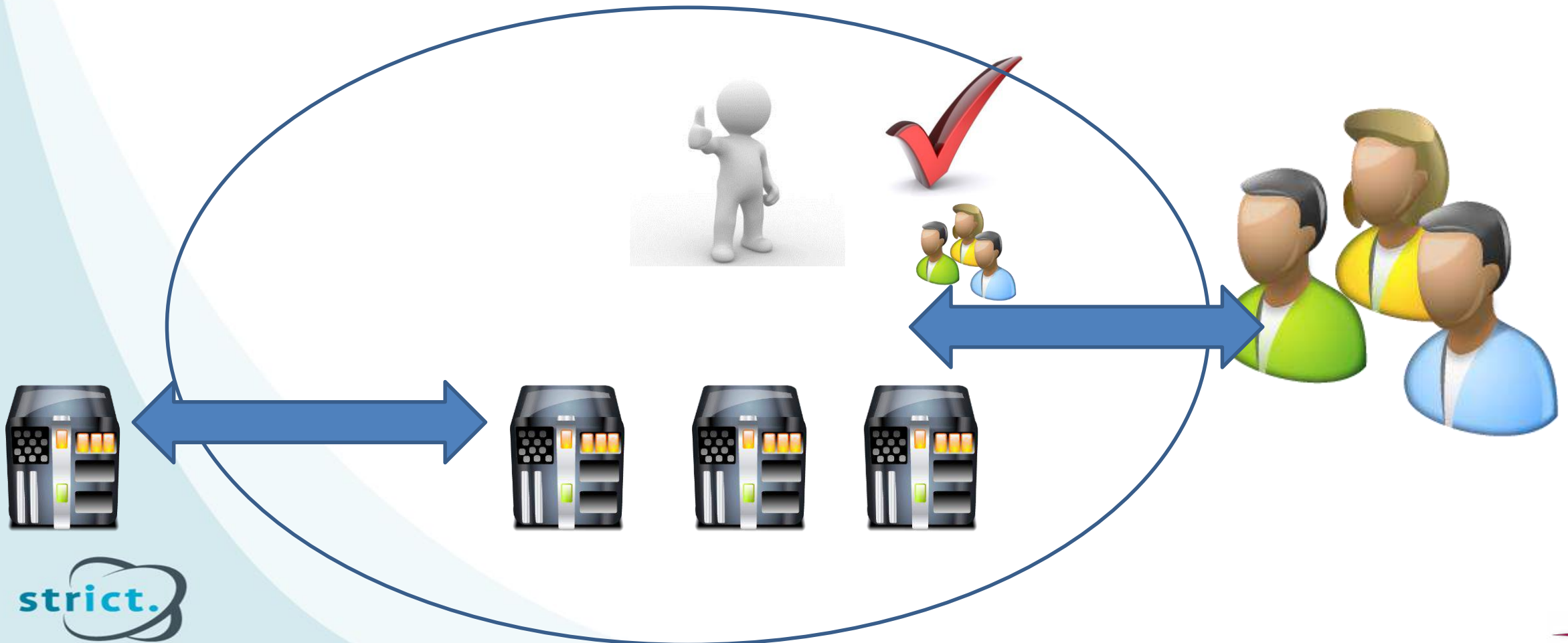


Op naar de cloud...



IAM 2.0

Federatie



Stork

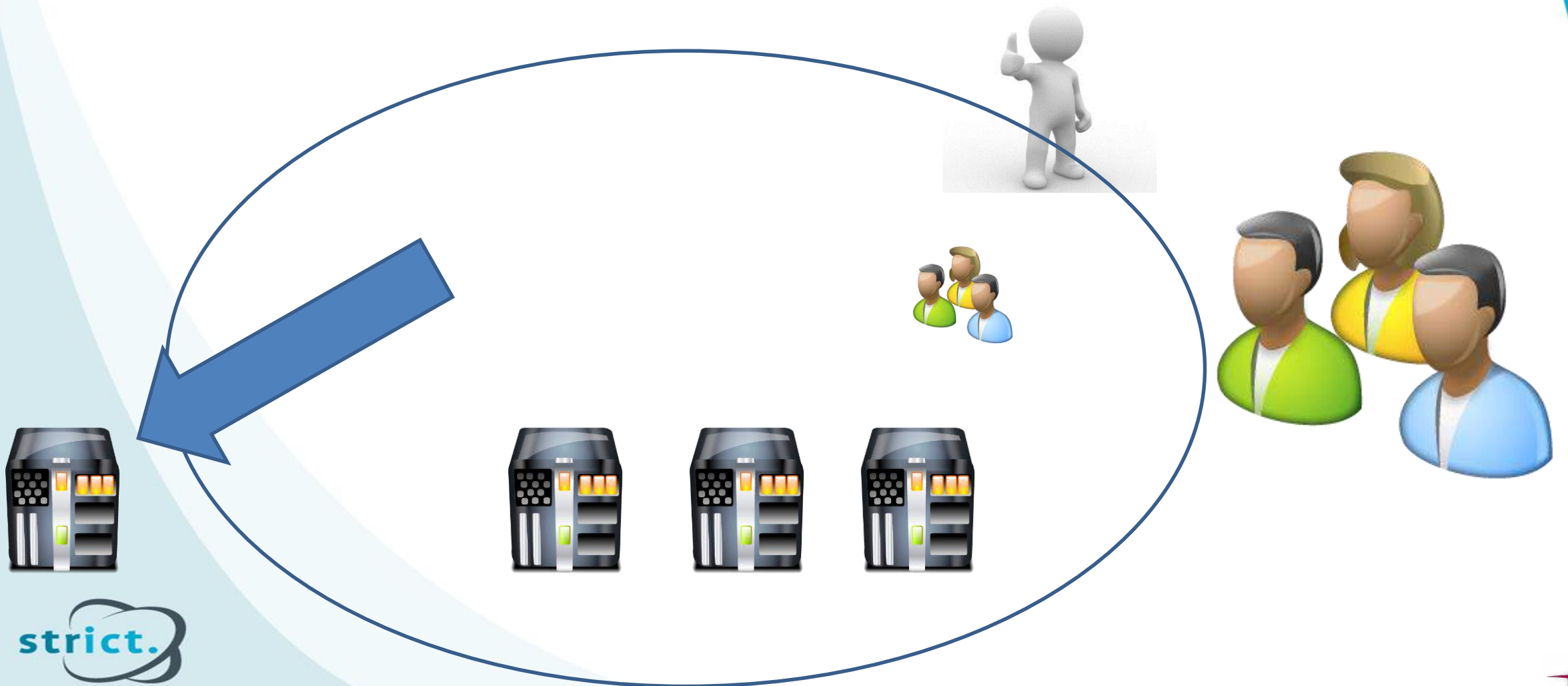


- STORK
 - Secure idenTity acrOss boRders linKed 2.0
 - <https://www.eid-stork2.eu/>
- 2 factors
 - Authenticatie bij registratie en uitreiking
 - Authenticatie tijdens gebruik

Stork QAA Assurance Level

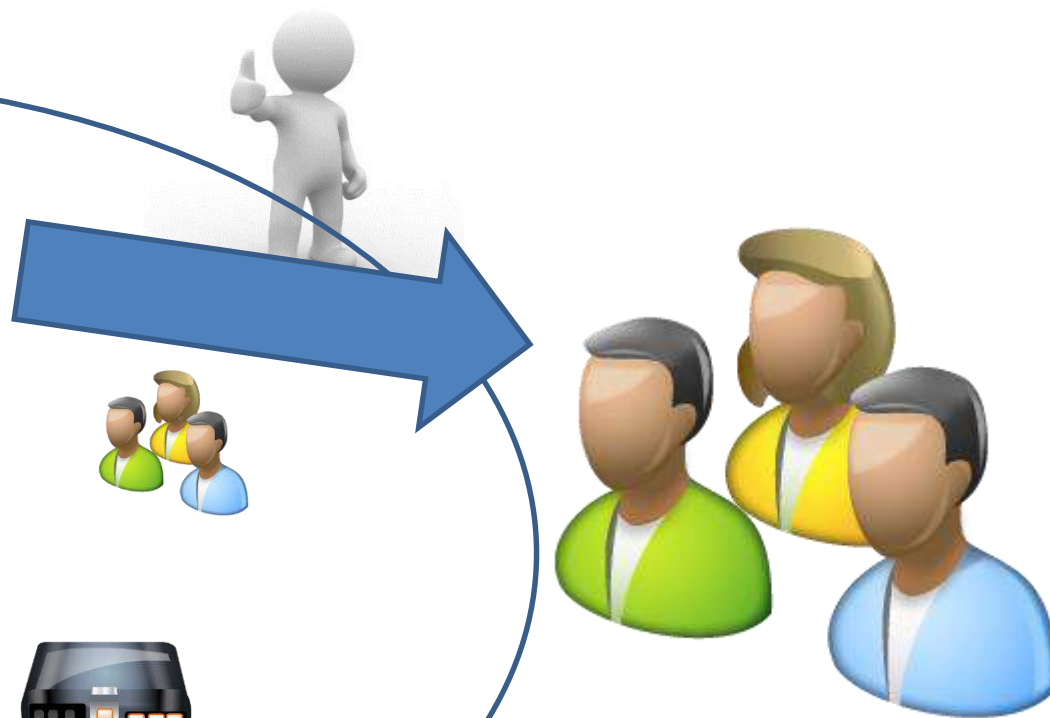
STORK QAA ASSURANCE LEVEL		Assurance level for the electronic authentication phase			
		EA1	EA2	EA3	EA4
Assurance level for the registration phase	RP1	QAA 1	QAA 1	QAA 1	QAA 1
	RP2	QAA 1	QAA 2	QAA 2	QAA 2
	RP3	QAA 1	QAA 2	QAA 3	QAA 3
	RP4	QAA 1	QAA 2	QAA 3	QAA 4

Kenmerken

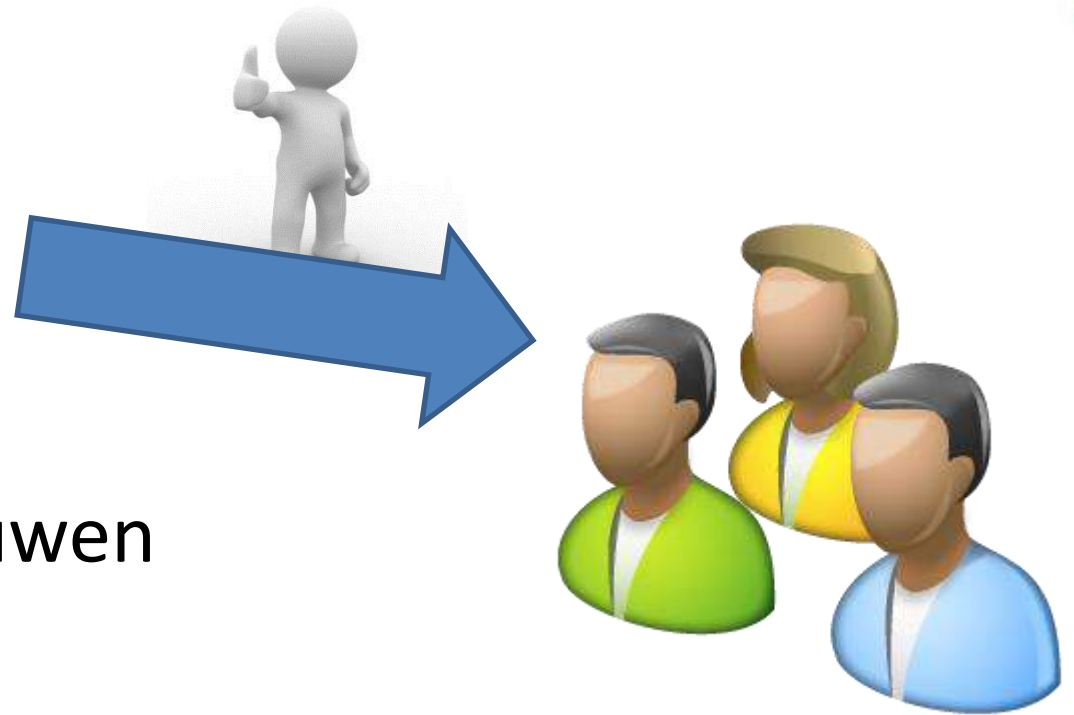




- Services
- Uitvoeren van taken
- Identiteit? Nee, competentie!

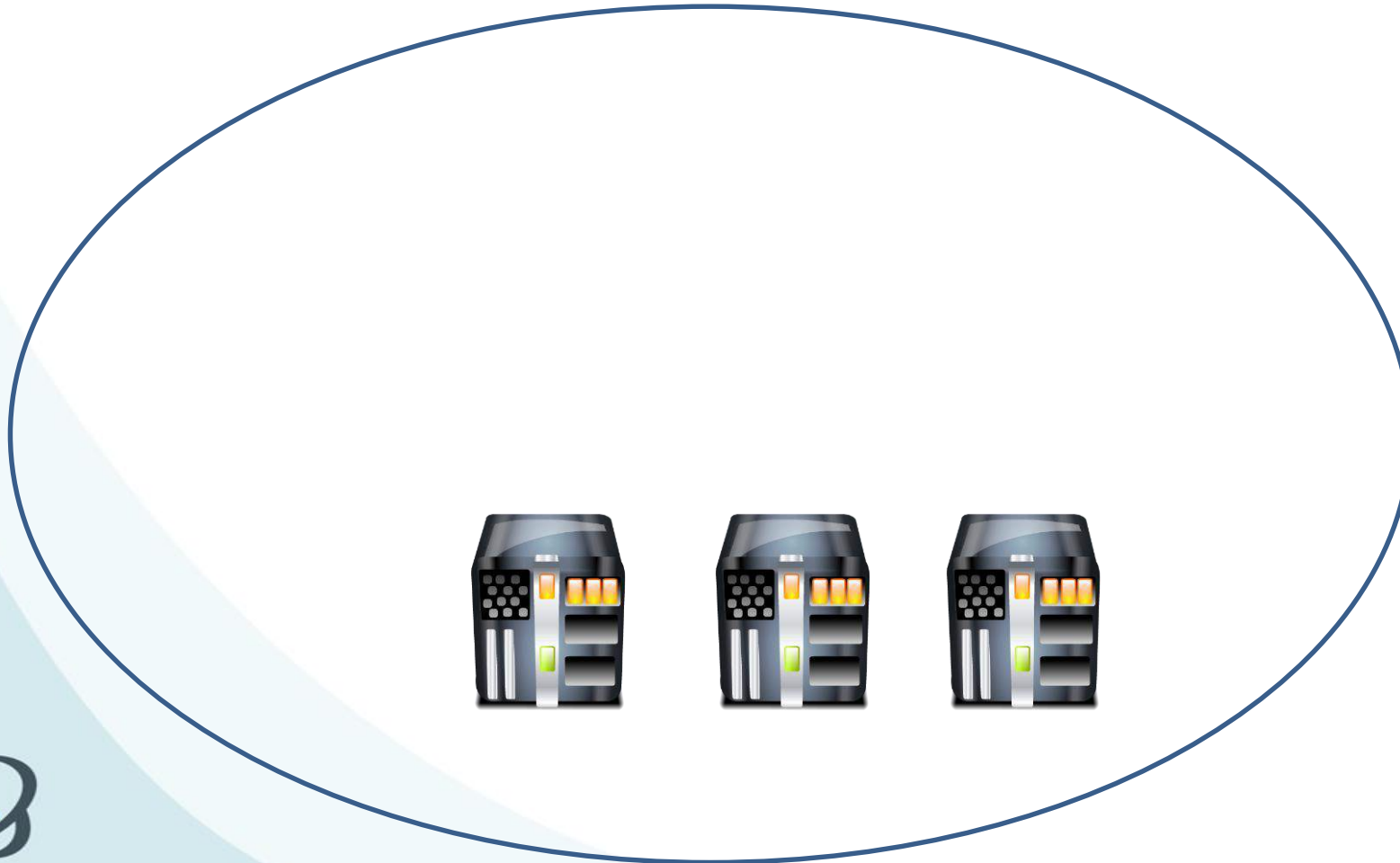


- Identiteiten
- Kenmerken van identiteiten
- Betrouwbaarheid en vertrouwen



IAM 3.0

Attributen



IAM 3.0

- Inzet van Identity As A Service providers
- Access Governance



- Proceseigenaar bepaalt criteria
 - ‘Wie’ niet relevant, ‘waarom’ wel
- Identity provider levert betrouwbare en vertrouwde attributen



Search for people, jobs, companies, and more...  Advanced

HomeProfileConnectionsJobsInterestsBusiness

Add organization

Certifications

Registered CyberXpert

@cyberxpert

Certified Information Systems Auditor® (CISA)

ISACA

Starting May 2014

Certified Information Security Manager® (CISM)

ISACA

Starting August 2006

Add certificate



André Koot



Here's where you tell the world a little about yourself and what makes you special. A brief bio can help you stand out from the crowd and give your profile some personality. [Enter your bio now »](#)

MY BADGES



Certified Information
Security Manager®
(CISM)
ISACA



Certified Information
Systems Auditor® (CISA)
ISACA



[Suggest a badge!](#)
Have an idea for a
badge you'd like to see
available on Acclaim?
We're listening.



André Koot



Share

Certified Information Security Manager® (CISM)

The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs.

ISSUED BY
ISACA

ISSUED TO
André Koot

ISSUED ON
19 Aug 2006

TAGS

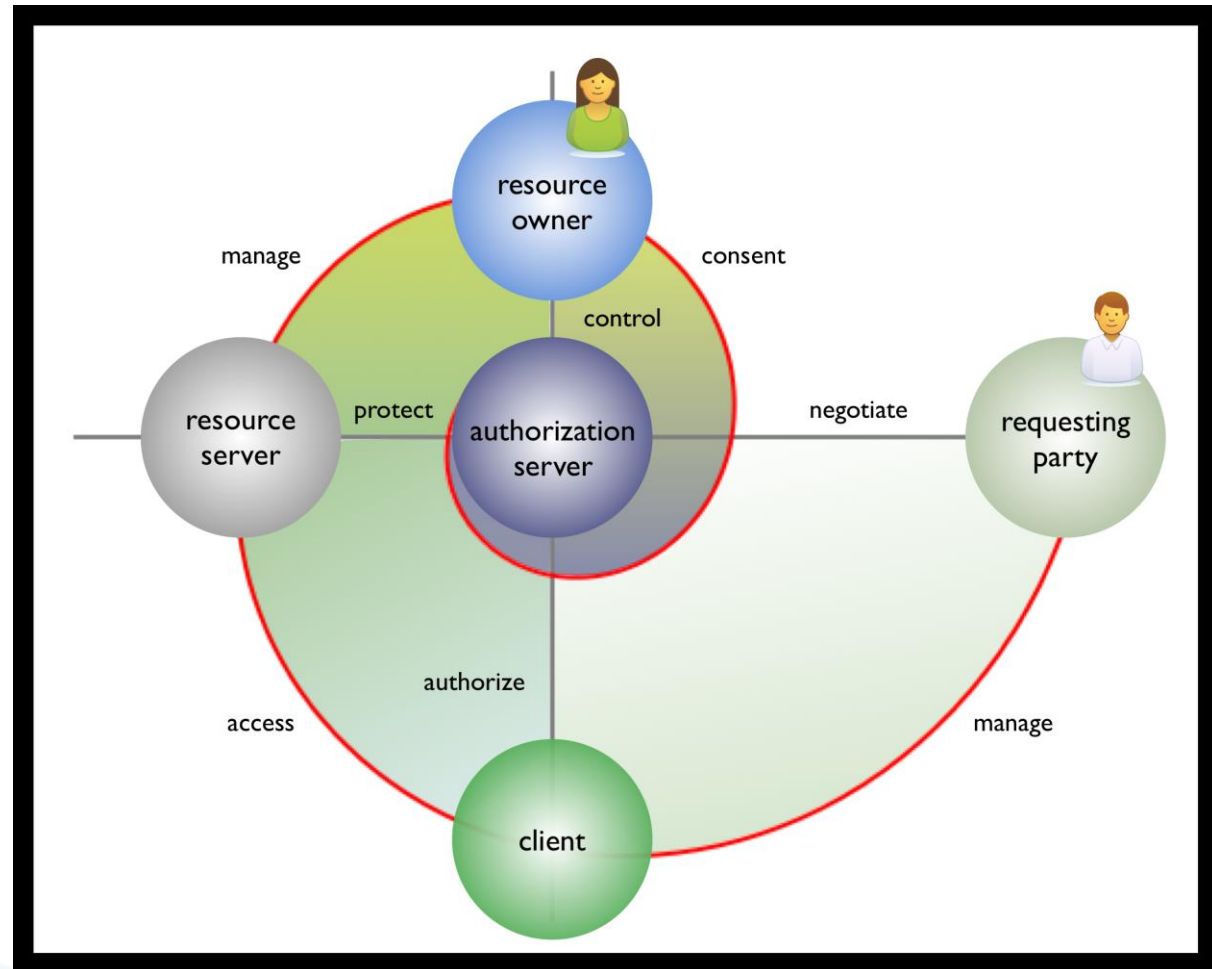
Information Risk Compliance Information Risk Management Information Security
Information Security Governance Information Security Incident Management
Information Security Program Development Information Security Program Management

WHAT IT TAKES TO EARN THIS BADGE

-  Score a passing grade on the CISM exam
-  Submit verified evidence of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice domains
-  Agree to abide by the ISACA Code of Professional Ethics
-  Agree to abide by the CISM Continuing Professional Education Policy

UMA

- User Managed Access



Wie ben ik

- De digitale identiteit
- Authenticatie
- Hergebruik

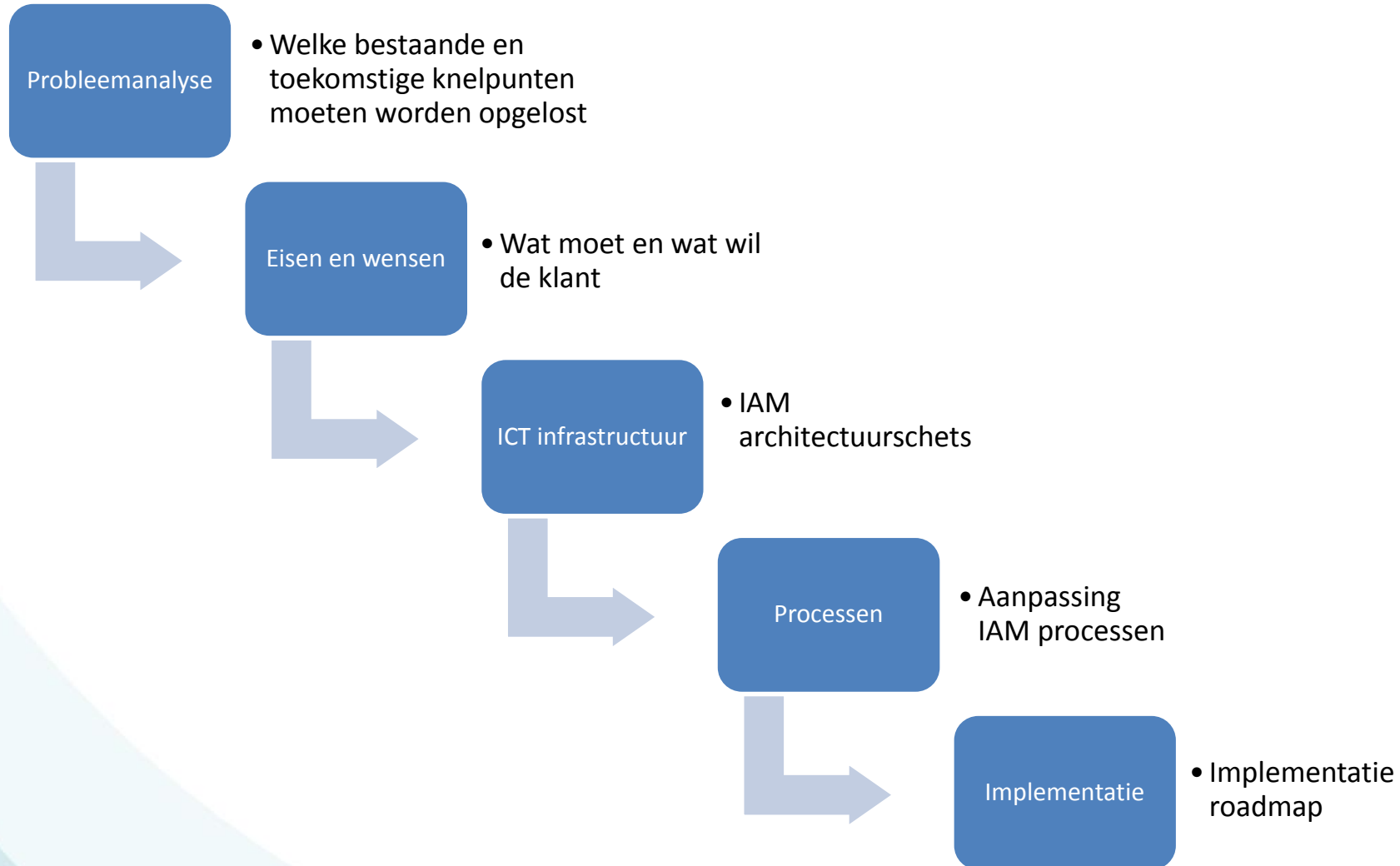
Wie ben ik

- De digitale identiteit
- Authenticatie
- Hergebruik

Mijn meest waardevolle identiteiten



De Strict IAM aanpak



Productselectie

- Markt...



Fig. 1: Overall Leaders in the Identity Provisioning market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].

Leverancier	Gartner	KupCol	Forrester	IDC	Regio	Platform	Db	Basis	Advanced	SSO	Extra / features	Markt	Lic
AlertEnterprise	V	-	-	-	US	Or/MS	x				SAP partner	l	COTS
Atos DirX	N	L	-	-	Eu		x	x			Kan ook Hosted	l	COTS
Avatier	N	C			US	NET	x					m	COTS
Avencis	-	C											COTS
Bay31	-	-					x						COTS
Beta Systems	N	L					x						COTS
Brainwave	-	-					x						COTS
CA Technologies	V	L				MS	x		x				COTS
Caradigm	N	-					x						COTS
Centrify	-	-								x			COTS
CloudID LionGate	-	-									Cloud	l	COTS
Courion	L	L					x	x			Business friendly	m	COTS
Covisint	-	-							x				COTS
CrossIdeas (nu IBM)	V	C					x					l	COTS
Deep Identity	N	C					x					l	COTS
Dell	V	L					x	x				h	COTS
Econet	-	-	-	-	De						SAP beheerscherm	l	COTS
efecte RM5	-	-	-	-	Eu		x				Finance	l	COTS
EMC RSA Aveksa	L	-	S	M	World	Java	Or	x		x		h	COTS
EmpowerID	-	L	-	-	Br	.NET			x			l	COTS
e-trust	N	-	-	-	Eu		x				Privacy oriented	l	COTS
Evidian	N	C	-	-	Eu	Java		x			RBAC enhanced, SMB?	m	COTS
Evolveum (Midpoint)	-	F	-	-	World	Java		x				l	Open
Fischer International	N	L	-	-	US	Java		x	x		Cloud	m	COTS
ForgeRock	-	L										h	Open
FSP	-	-	-	-	Re	Java		x			modern	l	COTS
GLUU	-	-	-	-	World	Java			x			m	Open
Hitachi ID Systems	C	L	-	-					x			m	COTS
IBM	V	L	S	L	World	Java		x	x	x	Maatwerk nodig	h	COTS
ILEX	-	C	-	-	Fr			x			SMB?	l	COTS
iSM Secu-Sys	N	C	-	-	De						SMB	l	COTS
ITConcepts	-	-	-	-	World					x			COTS
MacAfee	-	-	-	-	M	World							COTS
MicroSoft	C	-	-	-	NET	AD / MS					EOL?	h	COTS
NetIQ (voorheel Novell)	C	L	L	M	World	Java		x	x	x	Met Sailpoint	h	COTS
Netprof	-	-	-	-	DE						Education	l	COTS

Basisset
Provisioning
Reconciliation
Workflow management
Rapportage
Rollenbeheer
Gedelegeerd beheer
Wachtwoordenbeheer
User Self service
SAML protocol
Gebruikersportaal

Advanced
Access Governance/intelligence
Kritische accounts
Moderne Interfaces
Functiescheiding
Cloud provisioning

- Wereldspeler met Europese aanwezigheid
 - Betrouwbaarheid
 - Voldoende support
- Geen kleine partij
 - Ontwikkeling en continuïteit
- Betrekkelijk weinig maatwerk nodig
 - Kosten

