going from central to distributed identity in population scale trust ecosystems

DIACC - November 2016

DIGIDENTITY

INTRODUCTION DIGIDENTITY

- Merge real and online life identity management

- The user is in full and sole control of their data

- Committed to bring the best user experience to consumers around the world through innovative solutions

DIGIDENTITY

- Global verification and authentication capabilities

- Working for Dutch and UK government

- Extensive experience in Population Scale Trust Ecosystems

GLOBAL

- ISO and ETSI certified

- Working for NL and UK government

- Experience in developing cross-border standards, frameworks and delivery requirements

COMPLIANCE

- Identity - verification, authentication and access management

- eSigning - advanced and qualified digital signatures

- Certificates - advanced and qualified SSL and email certificates

PRODUCTS

DIGIDENTITY

eGov
Strategy

DIGIDENTITY

eGOVERMENT AND IDENTITY

An eGov strategy typically is about:

    Digital by Default
    Digital Inclusion
    Open Source
    Public private partnership (if you're lucky)
    Government Governance

But typically the Strategy doesn't look at:

    True Privacy-by-Design
    Open data
    Balanced Governance
    The longer term need for Identity and appropriate Levels of Assurance
    Applicability of existing identity standards (eIDAS, NIST, GPG/45)
    The wider use of Government Identity in a commercial or business context

DIGIDENTITY

KEY CONSIDERATIONS

- Is there a requirement for an identity programme to support current and planned online government services?
- What current and planned services need an identity ecosystem within federal and state services?
- Determine what key risks and threats need addressing
- What levels of assurance are required to support current and planned online government services?
- Determine applicability of existing identity standards
- Does a personal data ecosystem exist? What key data sets are available within the public and private sectors to support the required levels of assurance
- What is the the optimal, practical delivery and commercial models for an identity ecosystem
- Determine the appropriate design for an identity platform to support the scheme
- Are there applicable standards already available?
- The best structure for an identity programme
- How in the longer term a Government Identity ecosystem could be utilised in a wider commercial context

DIGIDENTITY

CENTRAL IDENTITY

- Citizen-2-Government
- Government owned
- No hub
- No re-use
- Outdated technology (legacy) with strong limitations
- Client-Supplier governance and relationship
- Needs endless funding

DIGIDENTITY

Why
standards

DIGIDENTITY

STANDARDS

- Public Private Partnership
- Federated Governance
- Multiple suppliers, often from different sectors or even countries
- Outcome based
- Re-use is key
- Standards enable interoperability and compliance

- Collectively agree on fraud prevention and *Identity Repair*
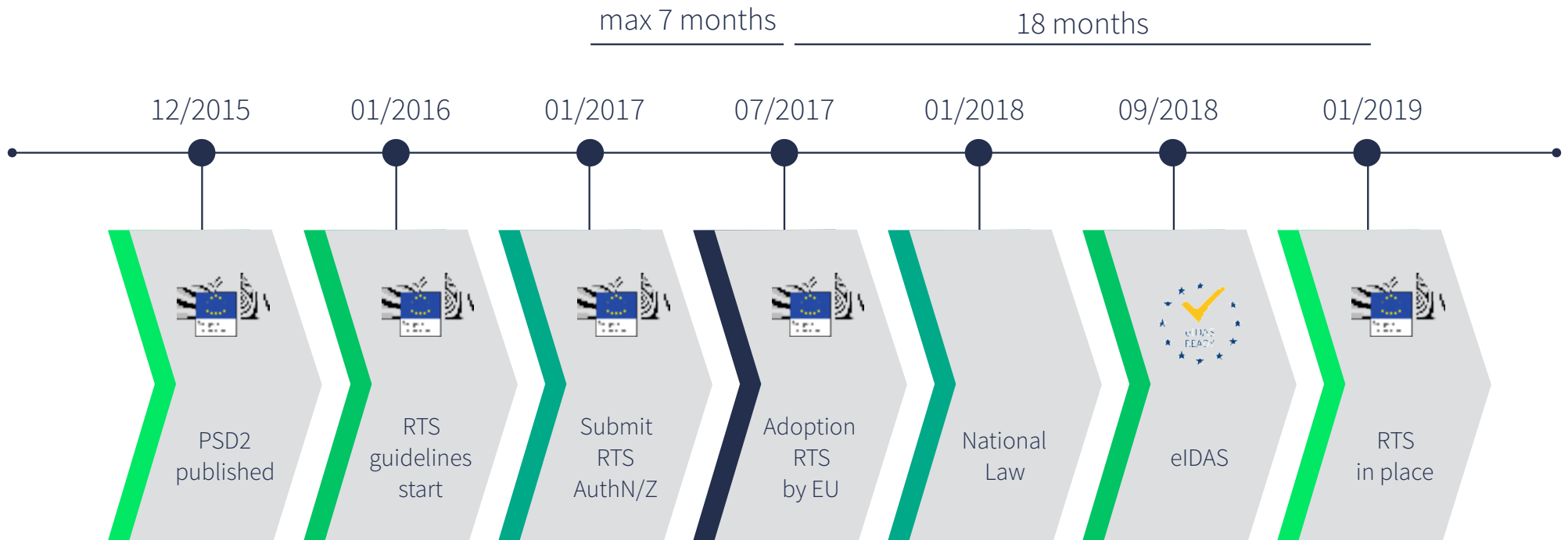
DIGIDENTITY

LESSONS LEARNED

- Government should drive *standards* and *outcome*
- *External assessment* based on international standards
- Adoption is based on success rate, *UX and benefits*
- Transparency and *iteration* to improve and evolve
- Business model needs to be *sustainable*
- Long term *commitments* are essential, from all involved

DIGIDENTITY

RE-USE

DIGIDENTITY

WHY RE-USE?

- Without re-use there is no sustainable business model for anyone involved

- What is re-use? The Identity or the Credential?

- Brings down price, increases awareness and adoption

- Build trust in a truly international ecosystem

- eIDAS brings Identity and Trust Services to a European level, with transparent requirements

DIGIDENTITY

COMPLIANCE ROADMAP

max 7 months

18 months

12/2015	01/2016	01/2017	07/2017	01/2018	09/2018	01/2019
PSD2 published	RTS guidelines start	Submit RTS AuthN/Z	Adoption RTS by EU	National Law	eIDAS	RTS in place

DIGIDENTITY

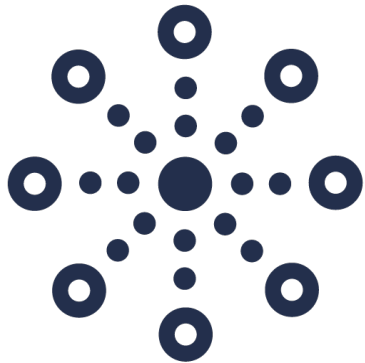# Identity Management

Marcel Wendt - Founder & CTO

DIGIDENTITY

Level of Assurance

A Level of Assurance is a combination of the
credentials (UK-GPG44)

&

the verification process (UK-GPG45)

eIDAS		LOW	SUBSTANTIAL	HIGH
EU STORK	LoA1	LoA2	LoA3	LoA4
UK	LoA0 / LoA1		LoA2	LoA3

DIGIDENTITY
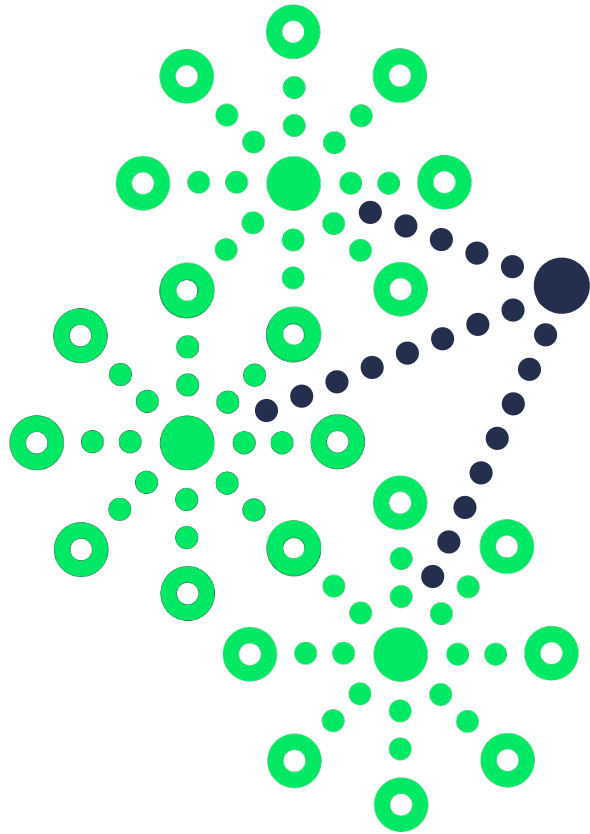
CENTRALISED MODEL

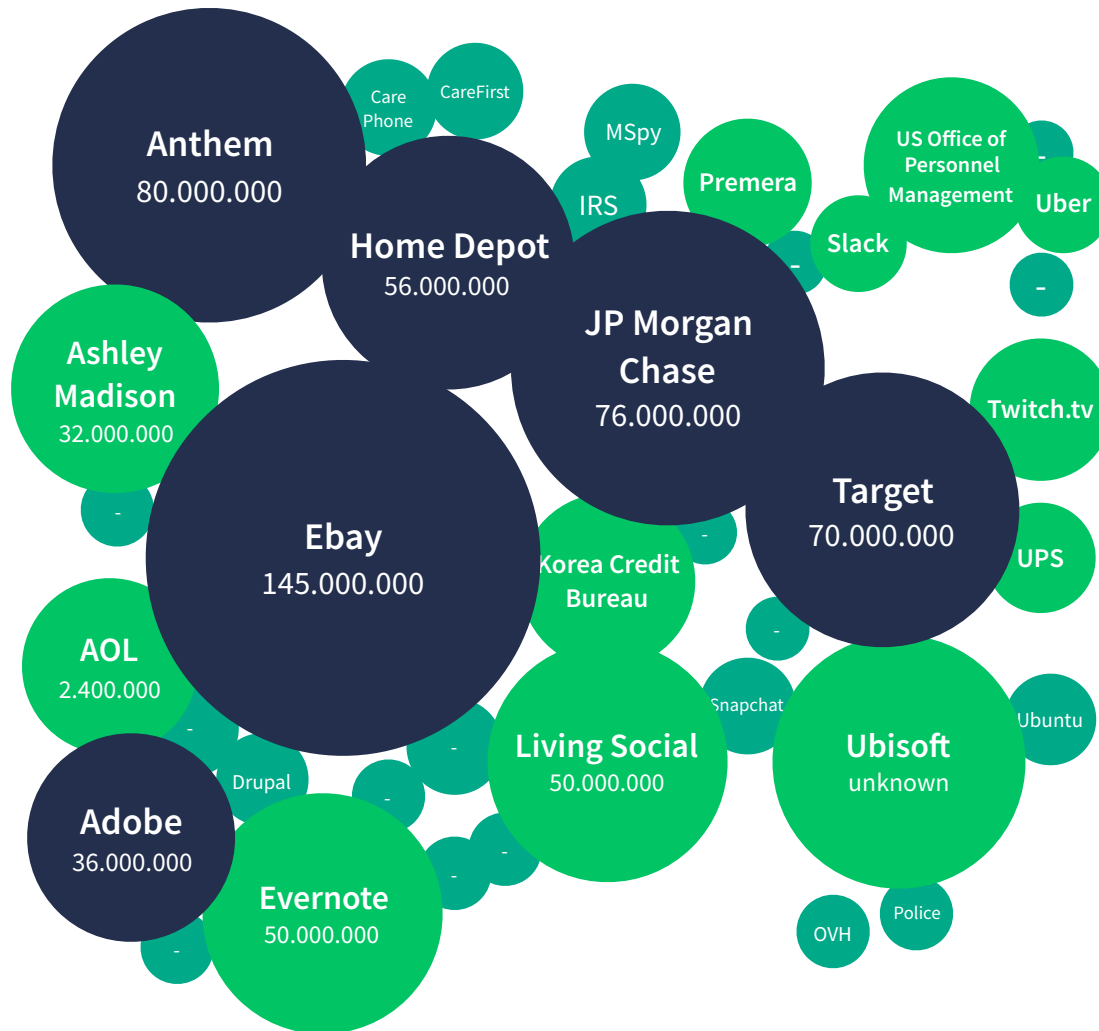| PROS	CONS
• Easy to connect to Napoleon databases; • One supplier but lock-in.	• Single Point of Failure; • Privacy Hotspot; • Often not Agile; • Blocks innovation; • One solution must fit many Citizens which results in legacy solutions like smartcard readers or simple username password with a low level of assurance.

DIGIDENTITY

FEDERATED MODEL

PROS	CONS
• No Single Point of Failure;	• Rely on attribute providers;
• No Hotspots;	• Maintain versioning over several IDP's;
• Implement Polymorph Pseudonyms;	• Fraud prevention mainly in isolation / on IDP level;
• Agile if your supplier is;	• Negotiate with and align multiple IDPs (commercials, standards, changes etc)
• Drives Innovations;	
• Many IDP's fits many citizens	
• Government becomes an attribute provider	

DIGIDENTITY

"THEIR" breaches exposing "US"

Anthem
80.000.000

Care Phone

CareFirst

Home Depot
56.000.000

MSpy

IRS

Premera

Slack

US Office of Personnel Management

Uber

-

Ashley Madison
32.000.000

JP Morgan Chase
76.000.000

Twitch.tv

-

Ebay
145.000.000

Korea Credit Bureau

Target
70.000.000

UPS

-

AOL
2.400.000

-

Snapchat

Ubuntu

Drupal

Living Social
50.000.000

Ubisoft
unknown

Adobe
36.000.000

-

Evernote
50.000.000

OVH

Police

ATTRIBUTE PROVIDERS

- eMail providers
- EU Mobile operators
  - 50% is PrePaid
  - 20% is Business
  - 30% has not 100% data quality
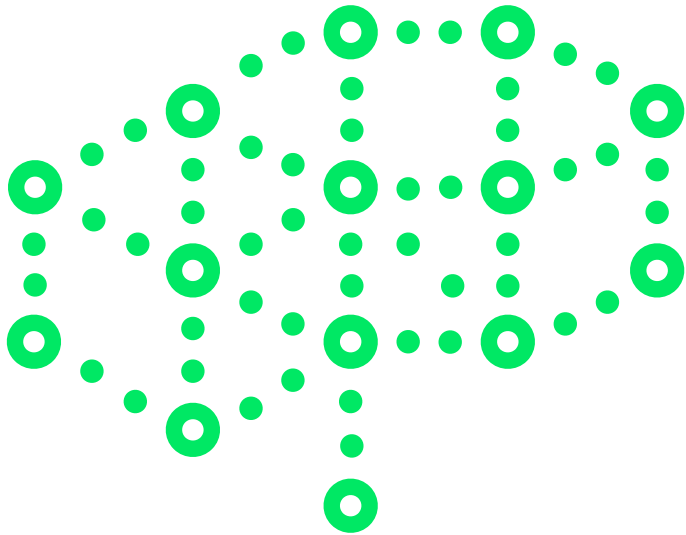- Knowledge Based Verifications

DIGIDENTITY

MULTIPLE PRIVATE HUBS

PROS	CONS
• privacy enhancing	• maintain versioning
• redundancy	• temporary excluding of an IDP
• central and local GOV	
• public an private sector	
• drives innovation	
• unified branding	

DIGIDENTITY

DISTRIBUTED MODEL

PRINCIPALS

1. based on the basic principal that it is an open ledger
2. the ledger is distributed and therefore exists in many nodes which removes the dependency of trusted 3rd parties
3. miners are special nodes in the network and their role is to validate and verify evidence (blocks) and add them to the ledger

Which all results in compliance upfront!

a million questions how to solve this…

DIGIDENTITY

KYC in a chain
to be continued....

DIGIDENTITY

DIGIDENTITY

Making life simpler and safer
by knowing who you are online

Waldorpstraat 17p

2521 CA The Hague

The Netherlands

+31 887 78 78 78

digidentity.eu

#digidentity_eu