HOW TO NAVIGATE THE REGULATION JUNGLE

- **Information security geek**
- **Privacy enthusiast**
- **IAM product manager**

JESSE KURTTO

1. A short look at the PSD2, GDPR, eIDAS and PCI-DSS 3.2
2. How Identity and Access Management can help you to comply
3. Go boldly where no one has gone before – Turn a regulation or directive into a business opportunity

GlobalSign GMO INTERNET GROUP

ABOUT US

GlobalSign is an identity services company providing cloud and on-premise IAM and PKI solutions for enterprises needing to conduct safe commerce, communications, content delivery and community interactions.

- Over 5000 Global partners
- Over 30 000 Customers
- 300 000 Companies use our IAM technology each month
- Over 10 years of experience in Identity and Access Management

GROUND BREAKING WORK BY DR. A. CAVOUKIAN

Research and 7 principles behind the concept “Privacy by Design”

Underlying framework for the General Data Protection Regulation, and many other initiatives

For information security experts… “Duh!”

- **Proactive**, not reactive; **Preventive** not Remedial
- Privacy as **default**
- Privacy **embedded** into Design
- **Full** functionality – Positive-Sum, not Zero-Sum
- End-to-End Security – Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy

PRIVACY BY DESIGN

https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

CROSSFIRE - OF REGULATIONS

The recent initiatives taken by the European Union have materialized as new regulation and directives. The payment industry has also taken steps…

PAYMENT SERVICES DIRECTIVE 2

TRANSACTION SECURITY

Financial transactions should use strong authentication

DIRECTIVE

Will need a local implementation

EUROPEAN BANKING AUTHORITY

Defines what “strong authentication” will actually mean –

by January 2017

GENERAL DATA PROTECTION REGULATION

PRIVACY BY DESIGN

New, strong privacy oriented regulation for the EU

REGULATION – NOT DIRECTIVE

No need to implement locally at the member state level

2018

Compliancy date May 2018 – Is your organization ready?

eIDAS

CROSS-BORDER FEDERATION BETWEEN EU MEMBER STATES

Use your own eID to access online services in another EU Member State

DIRECTIVE

Needs local implementation

PUBLIC vs PRIVATE?

Local implementation of the Directive will define if eIDAS is purely for public services or if private sector organizations can also participate

PCI-DSS 3.2

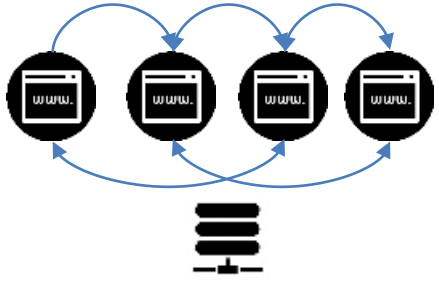
ACCESS TO CARD HOLDER DATA

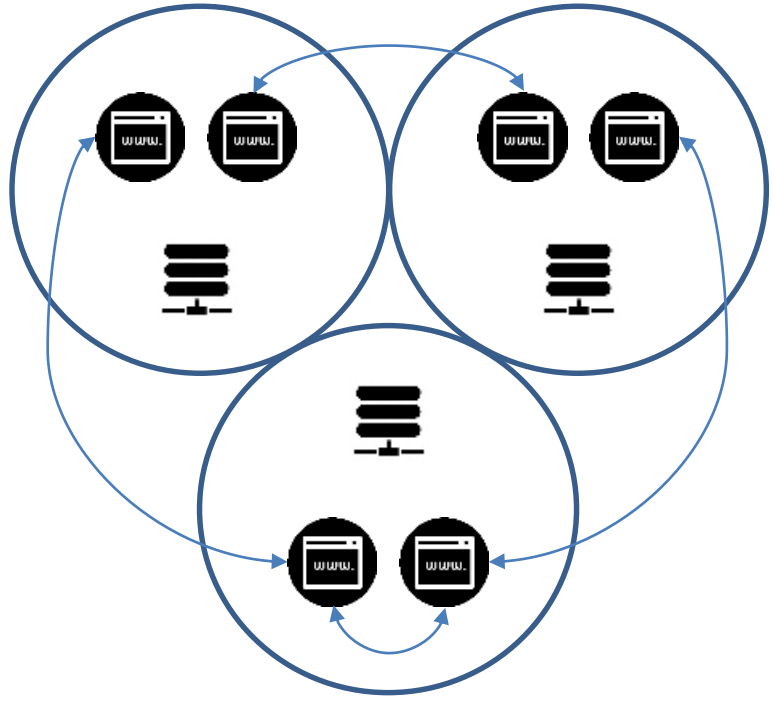
Access to the card holder data should be behind multi-factor authentication

INDUSTRY STANDARD

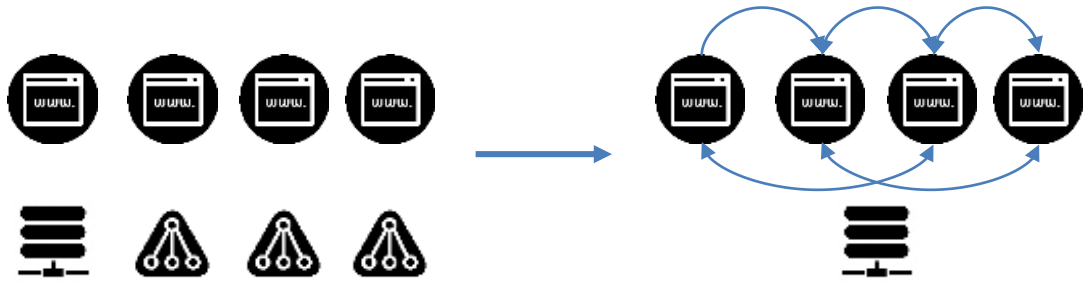
Everyone who handles credit card data should comply to this standard

MATURITY MODEL





FROM DAYCARE TO SCHOOL



CONSOLIDATE YOUR IDENTITY DATA

Moving from separate identity repositories to an IAM driven approach will help you

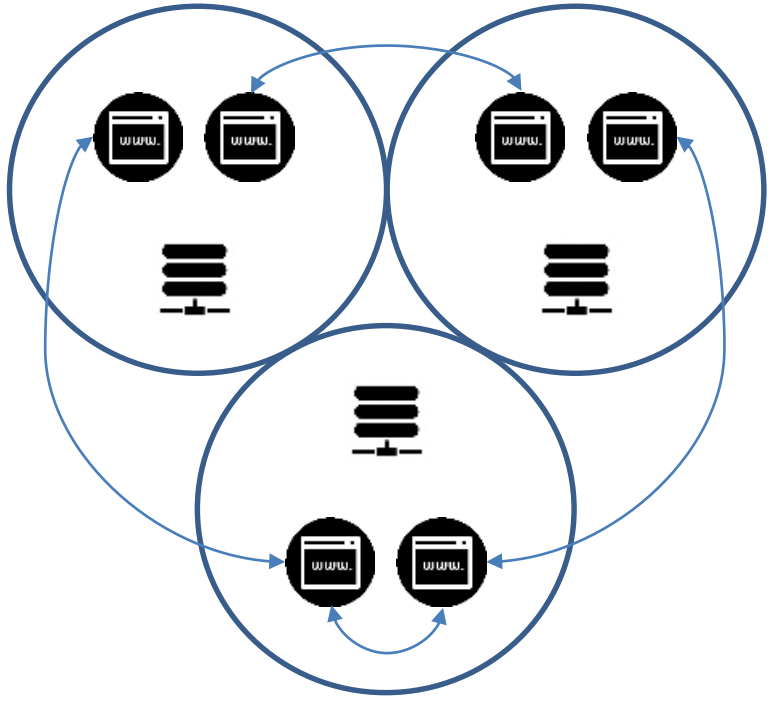
- ✓ Implement erasure of identity (personal) data [GDPR]
- ✓ Comply with data portability as you can now rely on a single data source [GDPR]

BUSINESS BENEFIT

Better customer experience, convenience, security

- ✓ Single Sign-On across applications
- ✓ Reduced number of access credentials (passwords?)

GRADUATION



FEDERATION AND BUSINESS ECOSYSTEMS

Standards based protocols for transferring identity information

- ✓ Disclosing the minimum amount of personal data to participants [GDPR]
- ✓ Consent driven – when moving between domains active consent is collected [GDPR]

BUSINESS BENEFIT

Build business ecosystems with your partners, customers, vendors, consultants etc…

- ✓ Single Sign-On across participants
- ✓ Cross-organizational customer acquisition

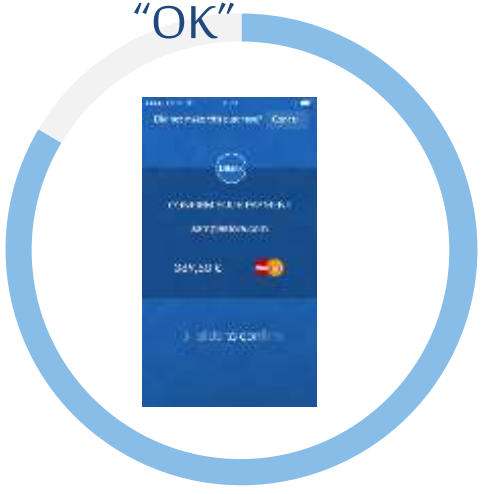
SECURITY

- WITH STRONG AUTHENTICATION

Strong, multi-factor authentication requirement is popping everywhere. From regulations to standards to simple customer demand

Level Of Assurance

"OK"



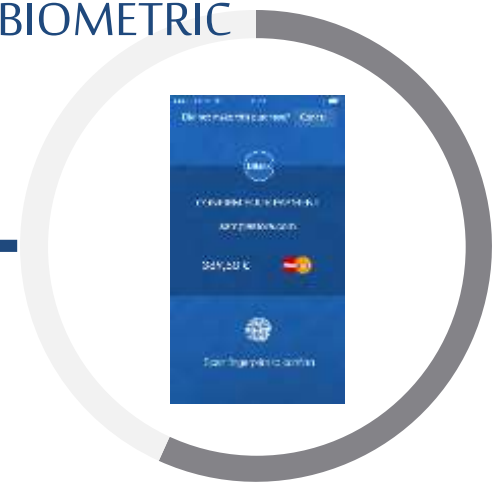
Authentication is based on the presence of the token (mobile device). Swipe, click ok etc…

OTP

One-time-passwords as an SMS message, mobile generated (offline), list etc…

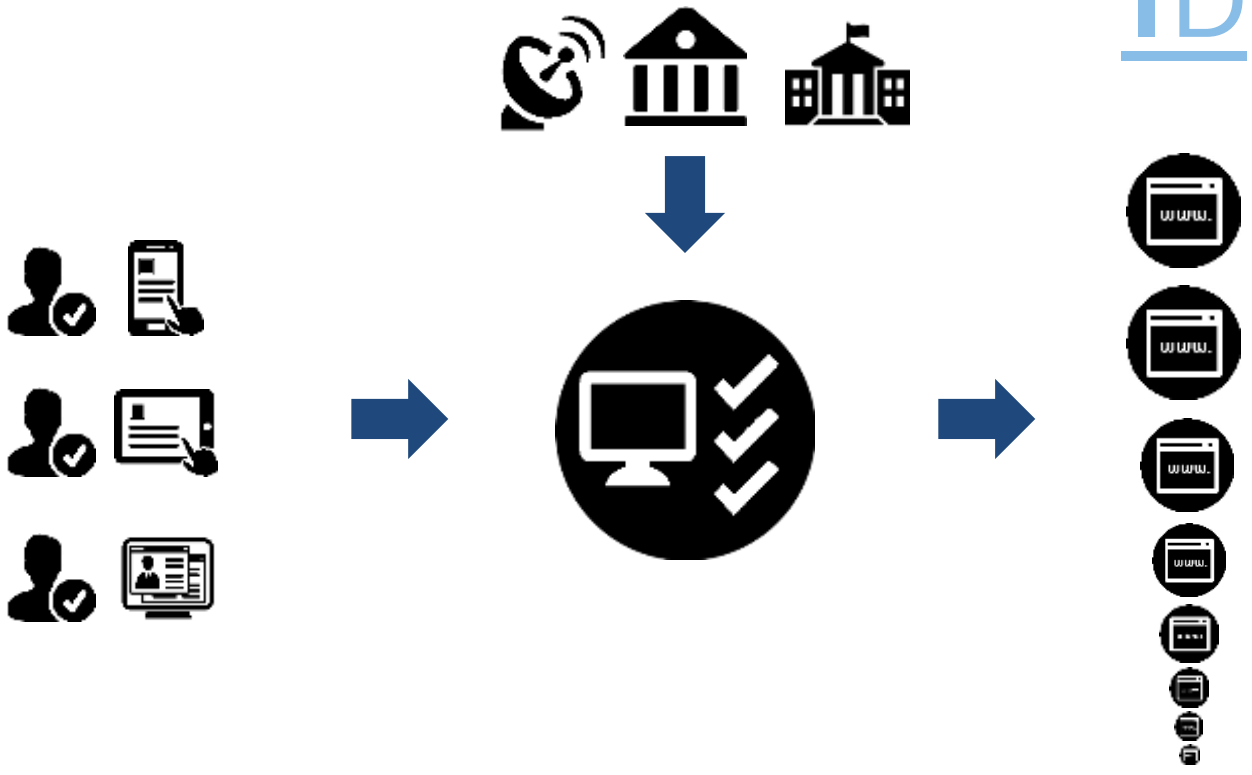
PSD2
PCI-DSS

BIOMETRIC



Fingerprint, facial recognition

IDENTITY PROVIDER



TRUSTED THIRD PARTIES

Utilize a strong credential issued by the government, bank or mobile network operator

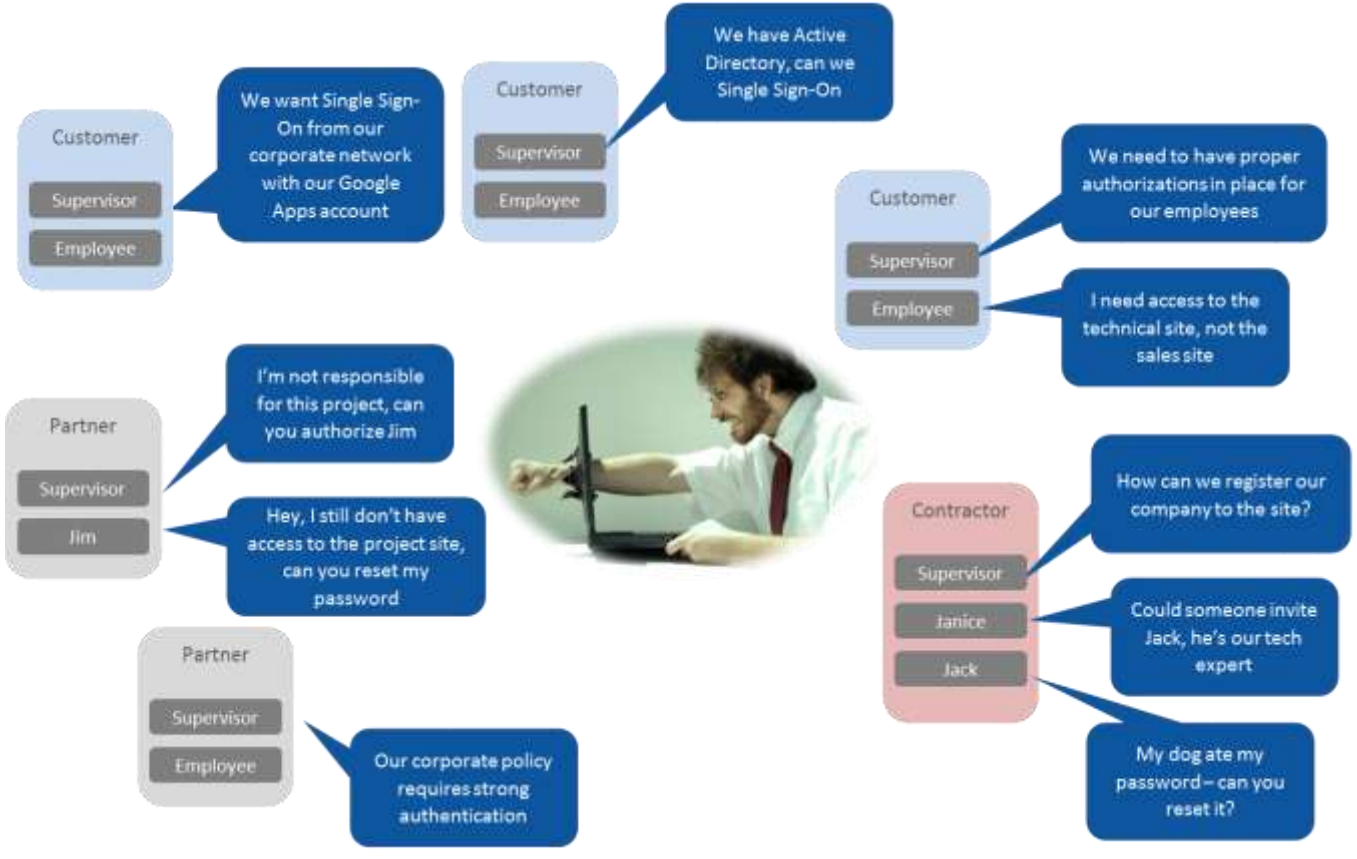
- ✓ Vetted identities
- ✓ In most cases providing strong, multi-factor authentication [PSD2, PCI-DSS]

LAUNCH YOUR OWN

Mobile app based (strong) authentication

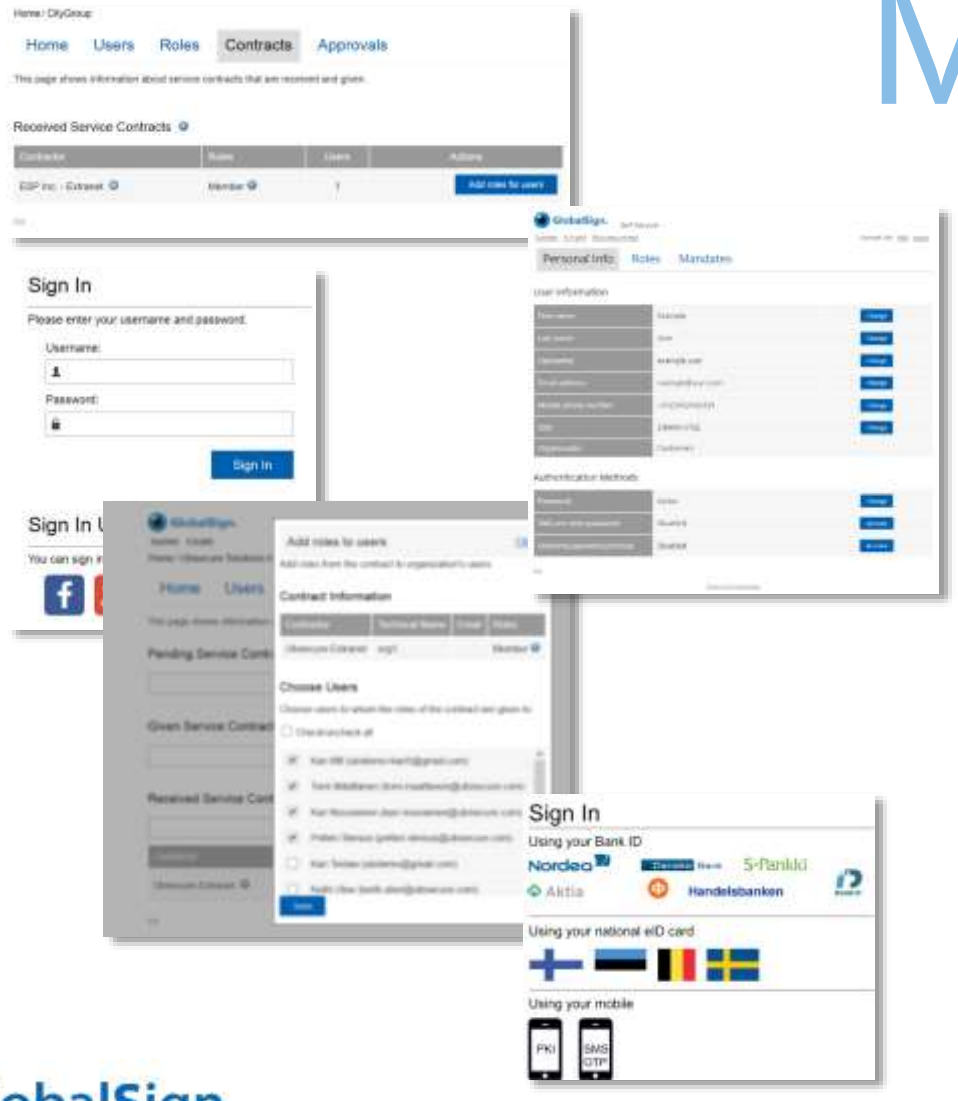
- ✓ TOTP, PIN, fingerprint, facial recognition
- ✓ iOS & Android
- ✓ Self-managed and self-printed OTP lists for fringe users (Blackberry, rotary dial, telegram…)

MANAGEMENT - PAIN



Management of customer or stakeholder data can be a pain – if you try to do it yourself. Let your external users manage themselves.

MANAGEMENT



SELF-SERVICE WORKFLOWS

Better control, visibility, transparency to the data you have on your customers

- ✓ Your users are managing their own information [GDPR]
- ✓ Your business partners can authorize their own employees and acceptance of an authorizations indicates active consent [GDPR]
- ✓ Considerable cost savings for your customer service operations
- ✓ Improved customer satisfaction
- ✓ Helping you digitalize your business in an effective and compliant manner

Information

GlobalSign, founded in 1996, is a provider of identity services for the Internet of Everything (IoE), mediating trust to enable safe commerce, communications, content delivery and community interactions for billions of online transactions occurring around the world at every moment.

US: +1 603-570-7060

FI: + 358 9 251 77250

UK: + 44 1622 766766

sales@globalsign.com

Mobile Connect contact: petteri.ihalainen@globalsign.com

Tel: +358 40 754 6363

www.globalsign.com

GlobalSign
GMO INTERNET GROUP