
asseco
DATA SYSTEMS

asseco DATA SYSTEMS

eIDAS & Blockchain
TSP Perspective

Marcin Szulga

Trust Services R&D Director

Asseco Data Systems S.A.

Certum by asseco

Asseco Group – global software producer

Nearly **30 years** of experience

Presence in over **50** countries

Listed on **stock exchanges** in Warsaw, New York and Tel Aviv

>100k clients use Asseco products

EUR 2.2 bn revenues in 2018

24,000 employees

EUR 187 m operating profit in 2018

> EUR 500 m dividends paid

20 LAT Certum by asseco

asseco DATA SYSTEMS

Experience | Security | Trust

6 continents
where Certum's services are

10 milion +
issued certificates

1 milion +
Online signature/seals per month

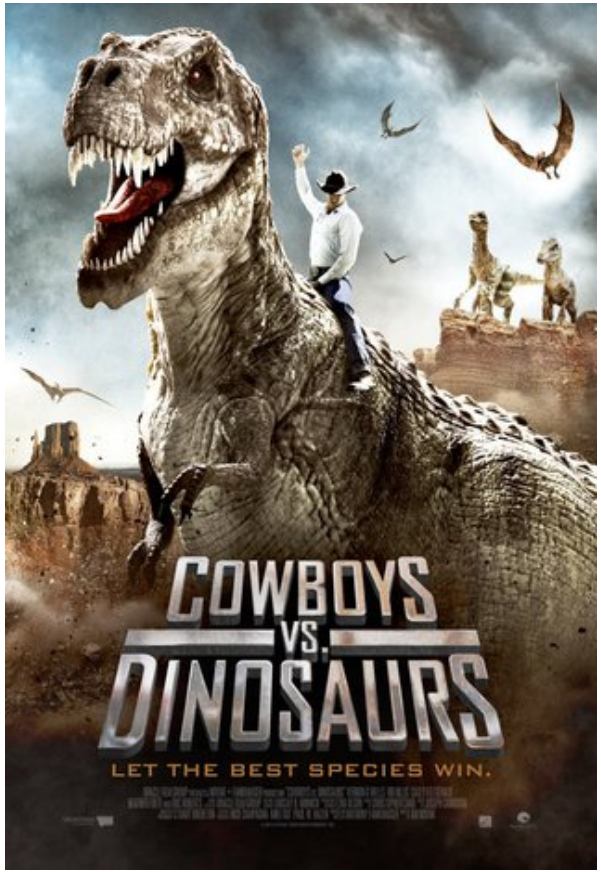
175 200 hours
of uninterrupted work

240 bilion inquiries
about the status of Certum SSL certificates annually

400 +
business partners worldwide

Blockchain Cowboys vs TSP Dinosaurs

asseco DATA SYSTEMS



Stuart Haber

W. Scott Stornetta

Stereotypes

DLT community loves innovations and focus to address business needs on large scale

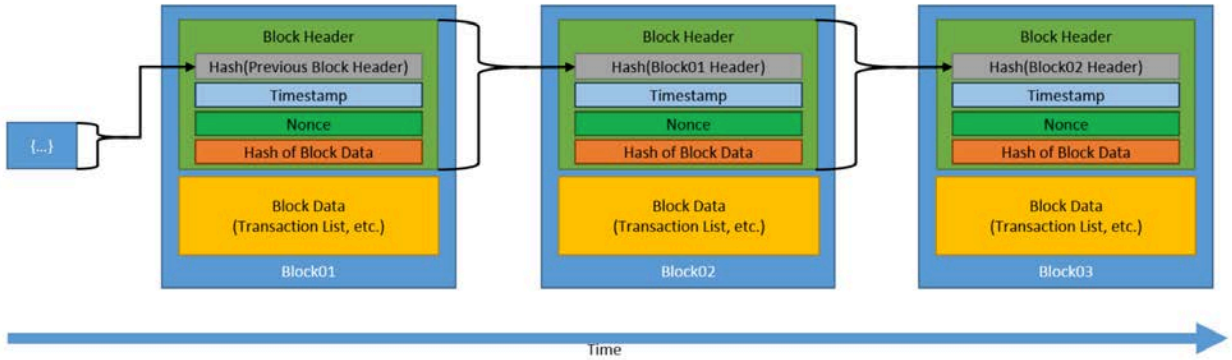
---

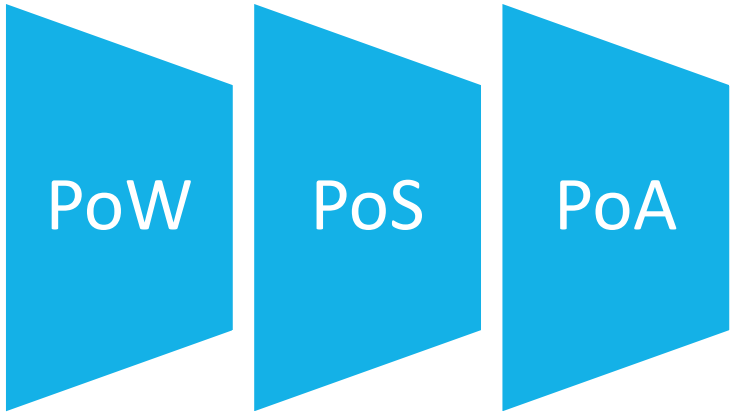
PKI Dinosaurs are risk focused, love compliance, governance etc.

Each community tends to overestimate their competences

Blockchain Basics

asseco DATA SYSTEMS





Source: NISTIR 8202 – Blockchain Technology Overview

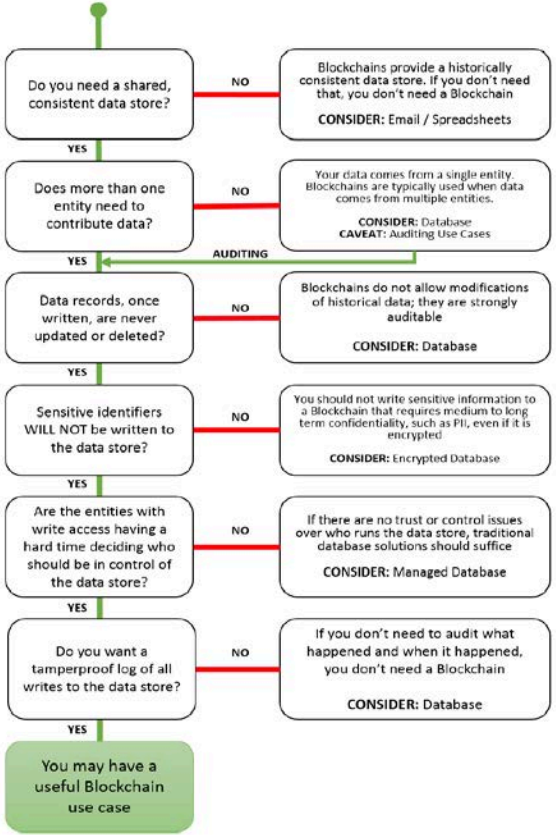
- Transaction electronically signed
- Transactions aggregated in blocks
- Blocks hash calculated , timestamped and chained with previous block

---

Which user publishes next block depends on consensus model.

Do we need a distributed ledger?

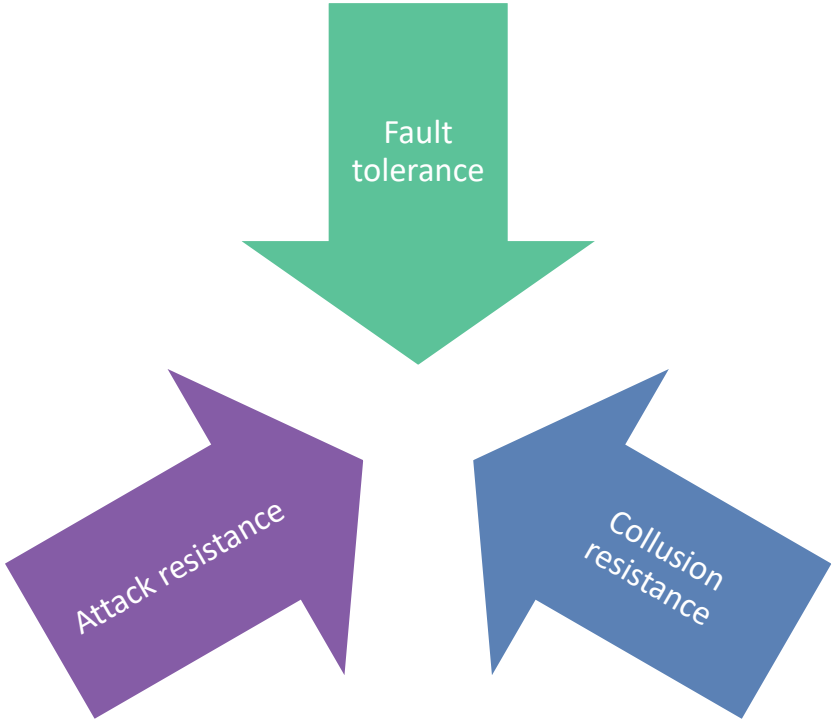
asseco DATA SYSTEMS



Source: NISTIR 8202 – Blockchain Technology Overview

Mature requirement analysis needed

Distributed Trust Model



Source: Vitalik Bulterin – The Meaning of Decentralisation

Key decentralisation drivers

Decentralization Types

Decentralisation of

	„Classical" Trust Services	Blockchains	Bit Torrent
Architecture	●	●	●
Governance	●	●	●
Logic	●	●	●

eIDAS & European Norms

Source: Vitalik Bulterin – The Meaning of Decentralisation

How many nodes process computations?

Who control nodes?

Is it a monolith from logical point of view (e.g. logically monolithic database)?

Decentralization Benefits – IOTA example

asseco DATA SYSTEMS

- **Highly Scalable -** Increased network activity decreases transaction settlement Times – Benefits of Tangle
- **Low resource requirements -** Designed for tiny devices, such as sensors and other IOT devices
- **Zero-fee transactions** – mutual exchange of computational power for assurance and validation

Issues

Centralised coordinator protecting against 34% attack

Bug happens – e.g. all transactions shut down in 2017

IOTA foundation can sweep user tokens to IOTA controlled addresses

---

Rookie mistakes - proprietary crypto vulnerable to differential cryptoanalysis

---

But it’s still very promising project!

Blockchain Misconcepts

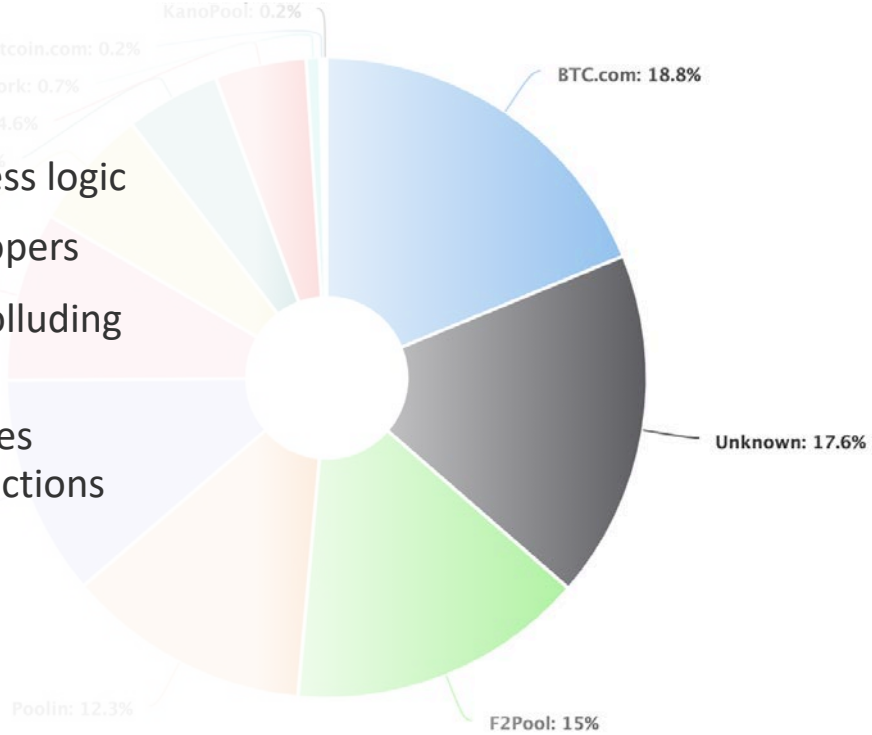
- **Immutability** – 51% attack
- **Governance** – software dev., publishing nodes, users
- **External Interfaces** – oracle problem (inconsistencies)
- **Services termination** – overpowering and replacing
- **Cyber attacks** – unpublished transactions
- **Malicious users** – short-term harm
- **Resource usage** – PoW
- **PKI and Identity** – 1:N:N relations (user, priv key, blockchain address)
- **SSCD, QSCD** – wallets in early development stage

Risk Analysis is crucial

Source: NISTIR 8202 – Blockchain Technology Overview

Blockchain Misconcepts

- **No trust** – “Trusted third party”



- ✓ Trust in crypto
- ✓ Trust in business logic
- ✓ Trust in developers
- ✓ Trust in non colluding in secret
- ✓ Trust that nodes process transactions fairly

Source: NISTIR 8202 – Blockchain Technology Overview, *Bitcoin.info*

There are trusted third parties in blockchain concept

Chaining is already present in Trust Services

- **Certificate transparency** – CT log ledger & continuous auditing principle
- **Long-term preservation** – appending the timestamps within centralized ledger

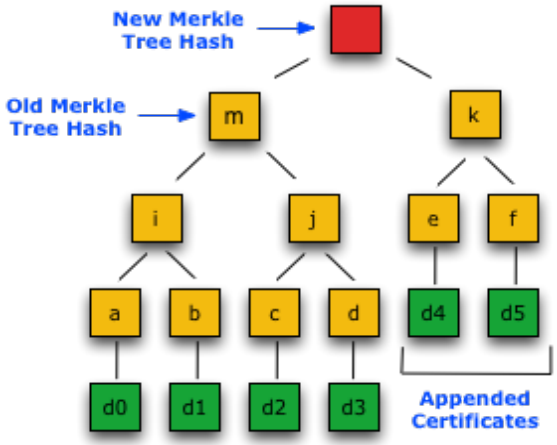


Figure 2

Source: http://www.certificate-transparency.org/log-proofs-work

Blockchain services governed by eIDAS

- **Electronic document Art. 46 –** Any content stored electronic form (definition no. 35).
- **If content is signed** – it's SES under eIDAS no matter how you sign. It falls under Art. 25.
- **Blockchain typically use digital certificates** - compliant with Art 26 – it's AES under eIDAS

CHAPTER IV

ELECTRONIC DOCUMENTS

Article 46

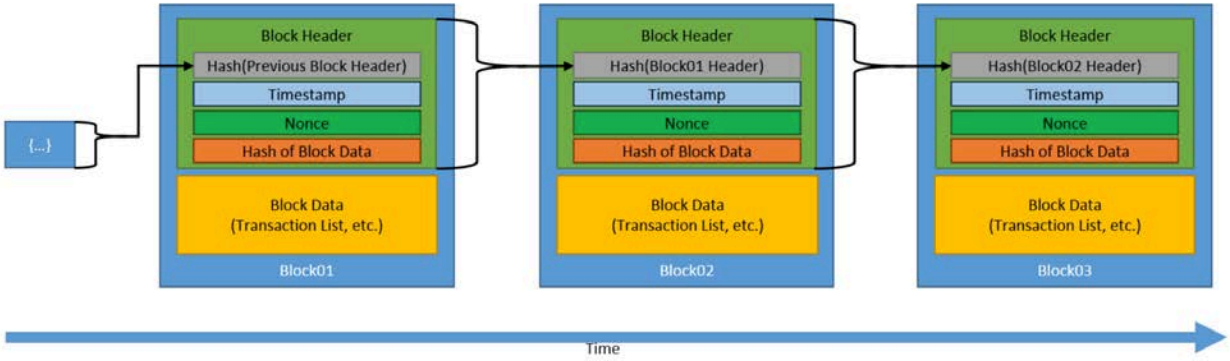
Legal effects of electronic documents

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

Blockchain's data compose an "electronic document". It's under eIDAS regulation.

eIDAS Trust Services in Blockchains

- **Electronic Signature, Seal** – transactions signing /sealing (on chain, off-chain (GDPR), pseudonyms (GDPR) or on private-permissioned ledgers (GDPR))
- **Timestamp** – timestamping the blocks
- **Validation** – transactions validation (signature, seal)



Smart Contracts use signatures seals to protect integrity of transactions or to electronically sign business logic uploaded to the ledger

---

Distributed Apps use signatures business logic

Timestamps incorporated in business logic brings Oracle (ledger inconsistency) problems

---

GDPR concerns – public certificates in transaction headers

eIDAS Services augmented by Blockchain

- **Distributed Digital Identities (DIDs)** – priv. keys under sole control (wallets) of individuals, augmented with additional (sensitive) attributes (attestations) issued by attribute providers and stored securely in wallets.
- **Revocation Transparency** - CRL Records
- **Distributed TSL** – Public permissioned ledger governed by Member States SBs and European Commission
- **QSCD Usage Transparency -** Remote QSCD audit log in Blockchain

`did:sov:3k9dg356wdcj5gf2k9bw8kfg7a`

Remote QSCD as an IoT device.

Ready for Qualified Trust Services on Blockchain (HLF)?

```
bccsp:
    default: PKCS11
    sw:
        hash: SHA2
        security: 256
        filekeystore:
            # The directory used for the software file-based keystore
            keystore: msp/keystore
    pkcs11:
        library:    /etc/hyperledger/fabric/DPoD/org1.example.com/libs/64/libCryptoki2.so
        pin: userpin
        label:
        hash: SHA2
        security: 256
        filekeystore:
            # The directory used for the software file-based keystore
            keystore: msp/keystore
```

- **Only P#11 interface supported** – QSCD Type 1 preferred
- **Only ECDSA supported** – Where are compliant QCAs?

PIN argument present in config file – no separation of credentials :/

Conclusions?

- **How do we address non-functional requirements in “old PKI" –** availability, scalability, performance, secure storage etc**.**
- **How do we deal with architectural (business) trade-offs on a daily basis? –** e.g. assurance level vs. performance
- **How do we support blockchain use cases for IoT –** are we ready for M2M scenarios? What about the “machine” sole control?

Let’s learn from each other!

Want to contribute?

asseco DATA SYSTEMS

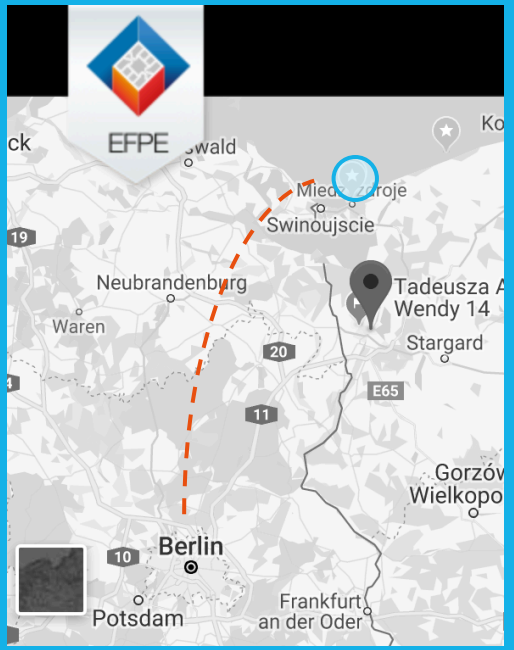
- **EU Blockchain Observatory** - https://www.eublockchainforum.eu/
- **Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL) -** https://www.etsi.org/committee/1467-pdl
- **CEN-CLC Focus Group on Blockchain and DLT**
- **ISO/TC 307** - Blockchain and distributed ledger technologies

EFPE 2020 - Trusted Economy

3-4 June 2020

Międzyzdroje

20 Anniversary ☺



Thank you.

Marcin Szulga

Trust Services R&D Director

marcin.szulga@assecods.pl

Asseco Data Systems S.A.

asseco DATA SYSTEMS

The power of creation.

www.asseco**ds**.pl

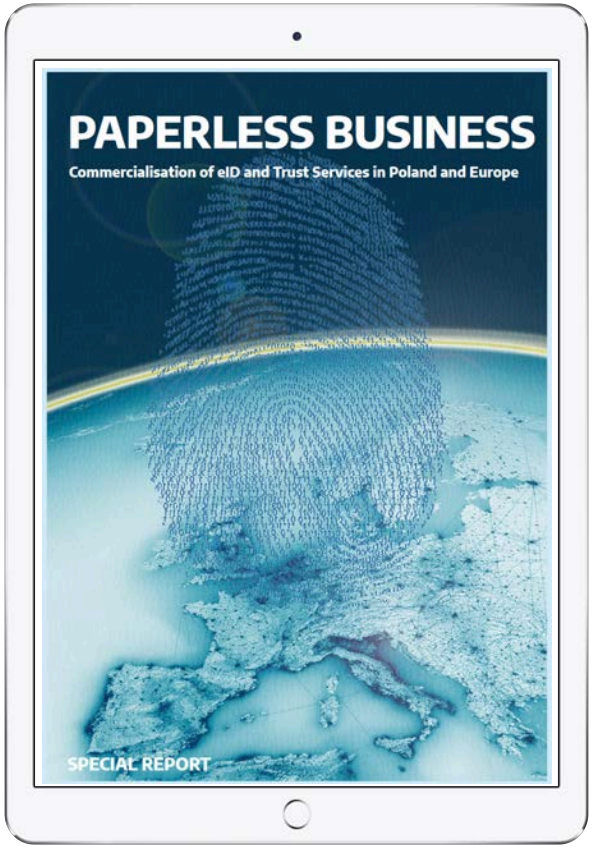
asseco
DATA SYSTEMS

OBSERWATORIUM.BIZ

PAPERLESS BUSINESS

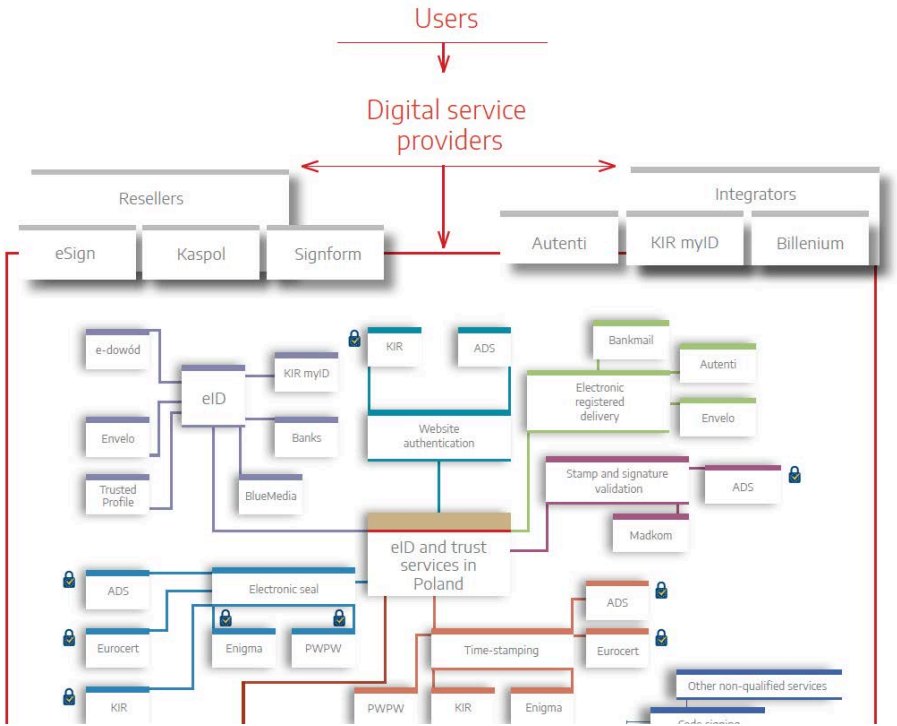
Report

September 2019



- **Report – PAPERLESS BUSINESS**
  - Map of eID and trust services vendors
  - European perspective
  - Commercialization of eID and trust services in Poland
  - Services & specific business needs
  - Business model
  - Perspective of growth

MAP OF eID AND TRUST SERVICES IN POLAND



- **Map of eID and trust services vendors**

  - Growing market of qualified services
  - New market of e-delivery and signature validation
  - eID – the Trust starts here
  - Emerging market of brokers
  - Growing role of users'perspective

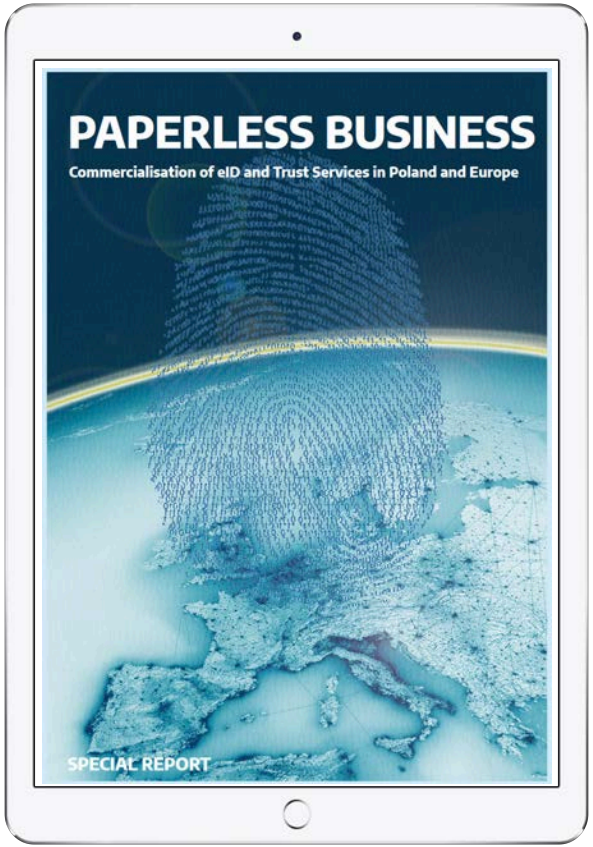
Key factors to success

1. Awareness of eID and trust services among digital service providers

2. eID/trust services availability and ease -of-use

3. Support from the regulatory environ-ment and its stability

4. Attractive business model for using eID and trust services



main patron
EFPE

scientific partner
C@ntrum
Prawnych Problemów Techniki i Nowych Technologii

social partner
POLSKA 5.0

partner
KIR

partner
asseco
DATA SYSTEMS

partner
SIGNICAT

partner
go.eIDAS

honorary patron
PIIT

honorary patron
MINISTERSTWO
PRZEDSIĘBIORCZOŚCI
I TECHNOLOGII

www.obserwatorium.biz

main patron
EFPE

scientific partner
C@ntrum
Prawnych Problemów Techniki i Nowych Technologii

social partner
POLSKA 5.0

partner
KIR

partner
asseco
DATA SYSTEMS

partner
SIGNICAT

partner
go.eIDAS

honorary patron
PIIT

honorary patron
MINISTERSTWO PRZEDSIĘBIORCZOŚCI I TECHNOLOGII

https://obserwatorium.biz/en/