A Comparison of Trust Models

Marc Sel

Royal Holloway, University of London
Marc.Sel.2013@live.rhul.ac.uk
Marc.Sel@be.pwc.com

Abstract

This article presents a comparative study of trust models, a term often used without a well-defined specification. Nevertheless, most automated enterprise processes rely on it. Examples include Automated Border Control gates, e-Government systems such as Tax-On-Web, electronic banking and money transfer and many more. We first present a short introduction to trust models. We then propose key terms to describe how trust can be established, and illustrate how these terms can be applied. Finally we compare the trust models created by ICAO PKD, EU eIDAS, US FICAM and Bitcoin, and present a conclusion.

1 Introduction

A key part of the development of the electronic society is the introduction of an economy based on electronic transactions and trust, as previously discussed, [1]. We consider trust as a factor that contributes to the taking of a decision. In cases as different as passing a Border Crossing Point, the ordering from a website, making a payment, or starting a medical treatment, trust will play a role in the transactions performed and decisions taken. In this context, an actor is an entity such as a natural or legal person that can act in one or more of trust-specific roles such as trustor, trustee and assessor. The trustor is the entity that is trusting. The trustee is the entity that is potentially trusted. The assessor provides claims about the trustee. Multiple assessors might provide claims about the same trustee. These assessors can have a varying degree of independence from the trustee. Also, a trustee may publish claims about itself. An artefact is a piece of electronic information produced by an actor (e.g. a certificate, an assertion, a time stamp, a claim, a signed document, or a list of trustees for a trustor). Obviously, many other roles can be considered.

Trust is based on elements as the existence (or lack off) of positive outcomes related to similar decisions taken in the past. We may have obtained these positive outcomes ourselves, or we may have learned about them from other sources that we rely on. Other elements include the extent to which some form of transaction-reversal is possible. The product or service provider may offer some form of guarantee or refund. Furthermore a regulator may force the provider to take liability.

Many solutions meet all reasonable expectations with regard to cryptographic trust in a PKI scheme such as appropriate key generation, subscriber registration, certificate creation and distribution, as well as publication of revocation information. All of these can be considered as relevant 'hygienic factors' that are required but not understandable by most end users. As a consequence, these hygienic factors don't necessarily contribute much to the trustor's perception of trust. Ele-

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2015), 1-10

ments such as reputation and an assessor's description or opinion on the trustee, formulated in a way understandable to the trustor, may actually contribute equally or more to this perception. Elements that introduce the notion of time into the trust evaluation equation will also contribute to this perception. An end user may trust an organisation more when it has a verifiable history of service provision. The gap between the safeguards that are in operation, and how they are perceived by users is referred to as the trust deficit.

The remainder of this paper is structured as follows. Section 2 elaborates the key concepts and terms we use to describe and compare trust models. In Section 3 we introduce some large scale trust models. This is followed, in Section 4, by a comparison of a selection of those. Section 5 describes related and future work, and Section 6 concludes the paper.

2 Key concepts and terminology

In most if not all instances where trust in electronic transactions is established, the following four types of trust components are involved: computational trust components (such as hard mathematical problems as the Discrete Logarithm Problem or finding points on an elliptic curve), technology components (such as Certification Authority servers, Hardware Security Modules (HSM) and On-line Certificate Status Protocol (OCSP) responders), operating procedures (such as face-to-face registration of an applicant that wants to subscribe to a CA's services) and compliance components. An appropriate combination of these components will yield legal effect.

There are many competing definitions and vocabularies for trust, indicating the concept's importance in many different scenarios and for different stakeholders. In the context of the present article we use the following terms:

- Trust model: a model of multi-party interactions that aims at facilitating a trustor's decision on the basis of metadata and services;
- Trust ecosystem: collection of trust models;
- Mechanism: the mechanism used to bind the participants within the model;
- Actors:
  - Initiator: the actor that took the initiative to create the trust model;
  - Governor/oversight keeper: the actor that governs the trust model and/or oversees it;
  - Operator: the actor responsible for the operation of the model;
  - Assessor: an actor that provides claims about participants;
  - Participants: actors that accept to be bound through the mechanism, this includes
    - Trust Service Providers (TSPs), actors providing trust services such as authentication, signature creation, validation, long term preservation, registered electronic delivery, time stamping etc. In such a context, the TSP can also be referred to as the trustee, the entity that is potentially trusted;
    - Subscribers, actors that subscribe to services offered by TSPs;
    - Relying parties, actors that rely on services offered by TSPs. In such a context, the RP can also be referred to as the trustor, the entity that is trusting.
- Metadata: data provided about the services and data used within a trust model.

3 Large scale trust models

We will now briefly describe some operational large scale trust models, based on computational trust. For an introduction, refer to the IETF's RFC 5217, [2], [3] and [4]. For an introduction to PKI trust calculus, see [5].

3.1 PKI single root model

In this model all participants rely on a single key pair, the root. The root's private key is typically used to sign subordinate public keys, resulting in a certificate chain that can be verified up to the root. The root's private key is usually protected by storing it in trustworthy hardware, and its public key can be verified by for example publishing its hash in a newspaper. Illustrations include electronic banking operating under a public CA or an internal Closed User Group set-up where the bank enrols customers and/or their devices in an in-house PKI, as well as government PKIs. PKI architectures such as the Belgian eID PKI have a single root which is used to protect separate subscriber certificates for authentication and signature. Other approaches to combination exist, e.g. SWIFT combines the SWIFTNET PKI, an application-level PKI, with a VPN PKI. Other large scale single root models include the Credit Card Schemes PKIs, and the European Root Certification Authority (ERCA) PKI architecture for the EU-wide digital tachograph.

3.2 Bridge CA model

In this model CA's are cross certified by a Bridge CA, which acts as an interoperability mechanism for ensuring trust across disparate PKI domains. Such a Bridge CA does not issue certificates to end entities (except those required for its own operations) but establishes unilateral or bilateral cross-certification with other CAs.

The *US Federal PKI Trust Infrastructure* contains the Federal Bridge CA. Successful cross-certification with the FBCA asserts that the Applicant operates in accordance with the standards, guidelines and practices of the Federal PKI Policy Authority (FPKIPA) and of the Identity, Credential, and Access Management Subcommittee (ICAMSC). Levels of Assurance range from 1 to 4, and are based on OMB M-04-04 and NIST SP 800-63-2. Also the *Transglobal Secure Collaboration Program (TSCP)* operates as a Bridge CA, dedicated to the defence industry.

3.3 Trust List model

In this model multiple CA's and their roots coexist at peer level. A list of root certificates is made available typically through a directory. All root certificates are at peer level, there is no hierarchy involved. The list itself may be signed by the publisher. Examples include the ICAO Public Key Directory (PKD), TeleTrust's European Bridge Certification Authority (EBCA), and the European List of Trusted Lists. In the ICAO PKD model, Country Signing Certification Authorities (CSCA) sign certificates of Document Signer Certification Authorities (DSCA). The latter sign the contents of electronic Machine Readable Travel Documents (eMRTD) such as e-passports. TeleTrust's EBCA publishes member registration and certificates via a Trust List based on ETSI TS 102 231. With its signature, the European Bridge CA confirms the origin of members' certificates in the form of a trust list. A similar model is used by the EU List of Trusted Lists (LOTL), which constitutes a supervised oligarchy. The European Commission publishes a signed list containing pointers to the Member State Supervisory Bodies. The latter publish pointers to the actual TSPs under their supervision.

3.4 Mutual Trust model

In this model all participants decide who to trust, and may convey trust information to other participants. While this model has its advantages such as the possibility for the participants to take their own decisions on who exactly to trust, it also places some operational burdens on them, and it scales more difficultly than a single root or oligarchy model. It is used by the Pretty Good Privacy (PGP) email system, and similar systems.

3.5 Other

Many variations of trust models exist. Examples include 'circles of trust' and 'hub models' in healthcare, where delegation is possible. The worldwide telephony system relies on trust between Home Location Registers (HLR) and Visitor Location Registers (VLR) to authenticate local and roaming subscribers.

Various systems introduce privacy features in a PKI setting. For example the Austrian approach to electronic identification includes a 'Source-PIN' (an undisclosed Personal Identification Number) from which sector-specific PINs are derived. The Source-PIN may only be stored on the citizen card, and is thus under the sole control of the citizen. In this manner, sector specific applications (including in the private sector) can derive their own ID numbers without giving them the ability to link data together. The Dutch Parelsnoer Biobank has a trust model that guarantees anonymity which can be conditionally revoked. In Germany, the electronic Personal Ausweiss (ePA) contains three different applications: "electronic identification (eID)", "Biometric application (ePass)", and "electronic signing (eSign)". Each application has its own trust model and is protected against possible misuse by access control mechanisms based on a dedicated PKI.

Furthermore Peer to Peer systems such as TOR, I2P, and Bitcoin have trust models without the concept of a central authority.

4 Comparison of trust models

We will now compare the trust models put forward by ICAO's global PKI Directory, the EU eIDAS regulation, the US FICAM model and Bitcoin's Blockchain trust model for virtual money. For this purpose, we first provide more details about each of these four trust models. Subsequently we compare them.

4.1 ICAO PKD

The ICAO PKD trust model is based on a Memorandum Of Understanding (MOU), signed by all participants. These participants are States issuing electronic machine readable travel documents (eMRTDs) according to the specifications of ICAO Doc 9303. An eMRTD's integrity is protected by a digital signature (referred to as Passive Authentication) supported by the following PKI components:

- Country Signing CA (CSCA): Every State establishes a CSCA as its national trust point in the context of eMRTD's. The CSCA issues public key certificates for one or more (national) Document Signers.
- Document Signers (DS): A Document Signer digitally signs data to be stored on eMRTD's; this signature is stored on the eMRTD's in a Document Security Object.

The States exchange CSCA certificates bilaterally or through the PKD Master Lists. The core trust services of the PKD are operated by Netrust, who publishes this list of CSCA Master Lists, as well as DS certificates and CRL revocation information.

Each State produces its own list of CSCA certificates that is relied on in the inspection process. Compiling this list is based on diplomatic exchanges and subsequent verification processes. A State may countersign its Master List of received certificates as part of the diplomatic exchange. It may publish this Master List to the PKD. CSCA Master Lists are compiled and signed by a dedicated Master Lister Signer. It is at the receiving State's discretion to determine the way it verifies and uses the received certificates.

For completeness, it should be mentioned that other PKIs are involved in eMRTD processing. Issuing States may include biometric features of the document owner and protect the access thereto by Extended Access Control (EAC) certificates. Furthermore, PKIs are used to secure communications between the various elements of the Inspection Systems front and back offices.

4.2 EU's eIDAS

In this trust model, described in [6], States may notify the European Commission of the electronic identity system they operate. As a consequence of this notification, the notifying State's electronic identities become recognised in the other States that already notified. For electronic Trust Service Providers (TSPs) it is possible to qualify their services. This results in supervision of the TSP by a Supervisory Body and in improved legal effect of the usage of these services.

The trust model is based on specifications (EU 910/2014 and ETSI), a compliance mechanism, and services provided by TSPs. The European Commission creates a signed top-level Trust List, referred to as the List Of Trusted Lists (LOTL). The LOTL contains pointers to the Supervisory Bodies in the Member States, who publish their national Trust List (TL). These TLs contain pointers to the TSPs under supervision, and their root certificates.

It can be observed that the eIDAS regulation ('Regulation of the European Commission on electronic identification and trust services for electronic transactions in the internal market', EU 910/2014) introduced the concept of a [Qualified] Trust Service Provider. However, the term 'trust' is not defined in the regulation. Rather, the term 'Trust Service' is defined in Article 3, (16). It can be summarised as electronic service normally provided for remuneration, which consists a.o. of creation, verification and validation of electronic signatures, seals, timestamps, registered delivery services and certificates, as well as certificates for website authentication and preservation services.

4.3 US Federal Identity, Credential, and Access Management (FICAM)

In this trust model, organizations that define a trust framework and certify entities compliant with it are called Trust Framework Providers (TFPs). Once a TFP has been adopted by the FICAM TFS Program, it then has the ability to assess and certify various identity services such as Token Managers, which provide the authentication functions; Identity Managers, which provide the identity proofing and attribute management functions; and Credential Service Providers, which provide a full service capability that combines authentication, identity proofing and the secure binding of token(s) to identity.

Identity services that have been qualified by a FICAM TFS-adopted Trust Framework Provider may optionally apply to the FICAM TFS Program to request approval for the authority to offer their identity services to the Federal Government. Applying to the FICAM TFS Program is optional because some qualified providers may not intend to provide their services to the Federal Government.

The *Authority To Offer Services (ATOS)* for FICAM TFS Approved Identity Services defines the process by which an Applicant, who has been qualified by a FICAM Adopted Trust Framework Provider (TFP) to meet FICAM Trust Framework Solutions (TFS) Privacy and Security requirements, can apply to the FICAM TFS Program to be approved to offer their services to the U.S. Federal Government. The applicant's responsibilities are then laid down in a *Memorandum Of Agreement*.

4.4 Blockchain model

The blockchain is the trust model underlying virtual currencies such as Bitcoin, as well as other innovative concepts such as the DNSChain, an alternative for DNSSec.

The Bitcoin trust model based is based on a combination of Elliptic Curve Cryptography (ECC) and what can be described as emergent convergence amongst peers through Proof Of Work (POW). Nodes compete in first finding a hash of a block of recently completed transactions, the candidate block. The hash should start with a number of zeros. To find such a hash, a certain amount of calculations must be performed, which constitutes the Proof Of Work.

It is inherently a P2P solution with a publicly available reference implementation of the standard node ('full node'). Such a full node includes a wallet, a miner, a full blockchain copy and network functionality. The wallet contains ECC keypair(s) and Bitcoin addresses, which are hashes of public keys. The miner contains functionality to build a candidate block and to compete for finding a nonce that will complement the candidate block's transaction content in such a way that the resulting hash of nonce and transaction content will meet the required difficulty threshold. The full blockchain copy contains all blocks up to the first (`Genesis') block. When a miner is the first to find the nonce for that candidate block, he can insert a new Bitcoin value of which he is the owner in the version of the candidate block that will become the next block in the chain. In this way the miner is rewarded for his work. Over time, the difficulty of finding the nonce increases because the hash has to contain an increasing number of leading zeros. And the new Bitcoin value that can be inserted by the winning miner decreases. The network functionality consists of P2P functionality to forward transactions and winning blocks within the network.

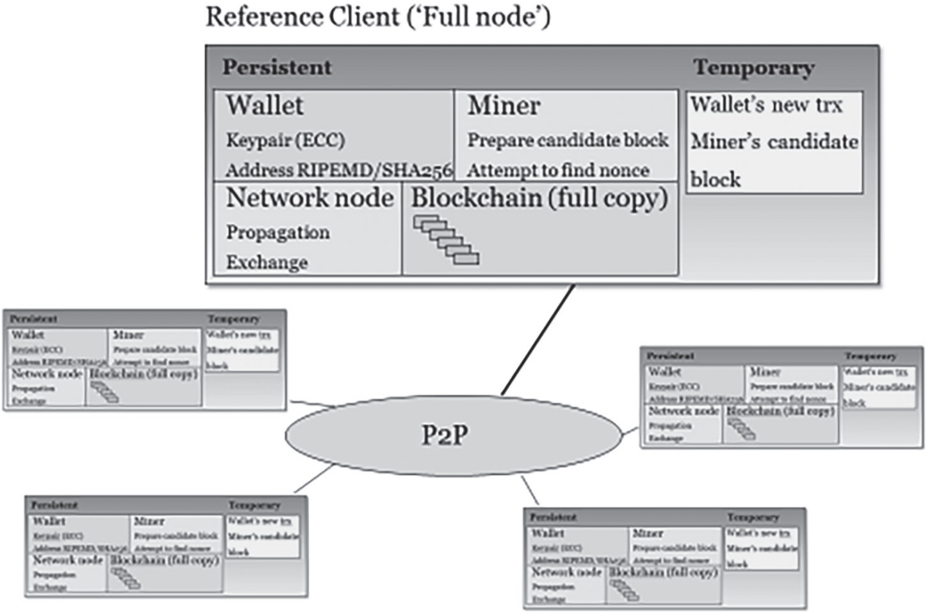

Figure 1: Bitcoin core model

In this trust model, following components contribute to trust. The Bitcoins include a digital signature with payer identification based on ECC. The publicly available blockchain can easily be verified by everybody, as hashes can easily be checked without a need for significant computing power or any external trust. As the blockchain contains the history of spending, a payee can easily validate that the Bitcoin has not been spent before by the same payer.

4.5 Comparison

The comparison between these four trust models is presented in the two tables below.

Table 1: a comparison of the different actors involved.

	ICAO PKD	eIDAS	US FICAM	Bitcoin (blockchain)
Actor: initiator	ICAO Council	European Commission / European Parliament (legislative)	Fed CIO Council (administrative)	"Satoshi Nakamoto"
Actor: governor/ oversight	PKD Board	EC/EP	OMB	P2P model with reference implementation
Actor: operator	Netrust (SG)	EC and Member States	GSA and TFS program	Individual nodes and exchanges
Actor: assessors	Self-assessment	SB, EA and CABs	GSA-TFPAP, TFP AAs	n/a
Actor: subscribers	Travellers from ICAO members	EU Citizens	C2G/B2G	Anyone
Actor: relying parties	IS of visited countries	Primarily PS	Fed Agencies	Anyone

Table 2: comparison of the other main attributes of these four trust models.

	ICAO PKD	eIDAS	US FICAM	Bitcoin (blockchain)
Objective	Worldwide authenticity of travel document & bearer	Enhance trust in electronic transactions (EU eID and Trust Services) for the Internal Market, for Natural and Legal Persons	US electronic Identity plus management of credentials and access, of NP for Federal Gov	Worldwide dematerialised money (fiduciary)
Mechanism	MOU	EU Regulation (mandatory for Member States) + ESO M460	FICAM Program (ICAM, FPKI, TFS, HSPD-12, FIPS 201) – "rules for participation"	Voluntary participation
Impacts	Participating States	EU-based IdPs that want to have their credentials recognised by MS public sector Relying Parties. TSPs that want their services to have legal effect.	US Fed Agencies and private sector TFPs that want to have their credentials trusted by US Fed Agencies	Payer/payees willing to accept bitcoins
Structuring principle	Participation by eM-RTD Authority (EMA)	Notification for eID (low, substantial, high), discretionary qualification of TS (electronic, advanced, qualified) with supervision	Authority To Offer Services (ATOS) through TFS program for service delivery to FedGov	Mining (finding a hashvalue that meets specific constraints)
Conformity mechanism	Registration procedure and test bench procedure	MS notification of eID to EC/MS SB registration in LOTL, MS SB's TL	TFS ATOS and TFP (OIX, Kantara, …) assessment	n/a
Supporting hw/sw/standards	ISO/X.509	ETSI/CEN M460	ISPPAP, NIST SP 800 series and FIPS 201 (PIV)	Compliance to reference implementation
Regulations	PKD Regulations	EU 910/2014 + IAs	FICAM (supported by SP 800-63) – FISMA (supported by SP 800-53)	Electronic money regulations
Machine readable information	Machine readable error codes for non-conformant entries in the PKD	LOTL and TLs	TFP metadata	Blockchain
Liability	ICAO MOU Art 6: ICAO exempt, participants for their own errors/omissions	Identity (Art. 11): in X-border trx, notifying MS, issuer, operator of the authentication procedure. Trust Services (Art. 13): TSPs	Identity proofing: CAB, but TFPAP limited to technical compliance	Own responsibility. When using a service provider, some contractual liability may be provided

4.5.1 Similarities

Many traditional large-scale trust models such as ICAO PKD, eIDAS and FICAM are organised as oligarchies, based on some form of a trust list. There is no single root of trust or a hierarchy.

Roles and corresponding accountability include initiator, operator, compliance assessor and participants. Segregation between these roles is common.

From operational and compliance perspectives, multiple layers of actors are involved. In the case of eIDAS, there is the Commission that publishes the LOTL, the Member State Supervisory Bodies that publish their Trust List, the Conformity Assessment Bodies that assess the TSPs. In the case of FICAM there is collection of TFPs and services provided compliant to these TFPs requirements, with compliance demonstrated via ATOS, TFPAP and TFP Assurance Assessors.

4.5.2 Differences

The main differences include:

- While eIDAS aims at establishing legal effect, US FICAM does not. US FICAM's conformity assessment is limited to technical compliance, legal consequences are out of scope.
- While eIDAS includes natural and legal persons, US FICAM is focused on natural persons.
- Most models have been created for a specific purpose in a specific context, and the trust established through them does not easily transfer to other circumstances.

The blockchain model as used by e.g. Bitcoin is inherently different from the other models described, as it is based on a combination of computational trust and a distributed transaction log verifiable by everyone, and no central point of trust. It can also be observed that the liability model is application-specific, and that Bitcoin has no liability model.

5 Related and future work

The exact functioning and role of trust models from vendors such as Microsoft or Adobe, as well as from the CAB Forum could also be analysed in a similar way. The trust models underlying Chinese and Russian trust ecosystems could be a topic of future research, as well as the interoperability between US, European, Chinese, Russian and similar trust models.

It can be observed that both in Europe and in the US, the concept of a Trust Mark is being introduced. Such a Trust Mark aims to provide assurance about the trust provided, by providing information on the conformance criteria and the conformity assessment process followed.

6 Conclusions

On a global scale, transactions are usually performed in an ecosystem that has no default trust mechanisms. The ICAO trust model and its oligarchy is an illustration how global trust can be established. As also illustrated by the eIDAS trust model, oligarchies are a common model for establishing large scale trust.

Large scale trust models such as US FICAM and eIDAS are composed of collections of trust frameworks, with segregation of duties between specifying, assessing compliance and operating the components that implement those frameworks.

Multiple large scale trust models co-exist and trust is being bridged across the individual trust models, as is illustrated by the mutual recognition initiatives by bridge CAs.

The emerging blockchain model is inherently different but holds great potential.

References

[1] Marc Sel. Using the semantic web to generate trust indicators. In Sachar Paulus, Norbert Pohlman, and Helmut Reimer, editors, Securing business processes, pages 106-119. Vieweg+Tuebner, Springer Science+Business Media, 2014.

[2] An overview of PKI Trust Models – Radia Perlman – IEEE Network November/December 1999

[3] NIST-SP-800-39 Managing Information Security Risk Appendix G Trust Models – 2011

[4] The Handbook of Applied Cryptography, CRC Press, 1997, Section 1.11.3 on trusted third parties and public-key certificates

[5] Jingwei Huang and David Nicol. A Calculus of Trust and its Application to PKI and identity management. In Proceedings of IDTrust 2009, April 14-16, 2009 Gaithers-burg, MD, USA. ACM, 2009.

[6] European Parliament DG Connect and European Council. Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. European Commission, 2014. EC 910/2014.