BLOCKSTAND

The role of the Decentralized Public-Key Infrastructure (DPKI) and its significance in enabling global trust and interoperability through blockchain technology

Erik Andersen
era@x500.eu

Relationship with current public-key infrastructure (PKI)

Rec. ITU-T X.509 | ISO/IEC 9594-8 (ITU-T X.509) provides the framework for public-key infrastructure (PKI). ITU-T X.509 is one of the more important cybersecurity standards being widely used for securing banking, health, e-government, etc., and lately also used within other areas such as the power industry and Internet of Things (IoT). ITU-T X.509 is also important in the context of Cyber Resilience Act (CRA). Item 24 from Annex I of the EU standardization requests for CRA mentions PKI explicitly. ITU-T X.509 is a horizontal standard, although item 24 is mentioned under vertical standards. PKI is the foundation for numerous vertical cybersecurity standards. The first edition of ITU-T X.509 was published 1988 as collaborative work between ITU-T and ISO/IEC. The nineth and latest edition of ITU-T X.509 is available here.

Establishment of global trust

PKI has served well where trust can be established by a so-called trust anchor trusted by everyone in a PKI domain. However, it has proved difficult or impossible to establish a global trust for a wider area with several interconnected PKI domains. There is an increasing need for having a Pan-European or even a worldwide set of interconnected PKI domains establishing a global trust. The solution for establishing a global trust seems to be trust by consensus rather than on local trust anchors not trusted in a wider context. Having a global trust by consensus implies the use of the blockchain technology for interconnecting PKI domains. This is the approach taken by Decentralized Public-Key Infrastructure (DPKI).

An International Standard

DPKI will be published as an International Standard issued as common text by both ITU-T and ISO/IEC. As an international standard, DPKI must follow the rules for international standard development. There are currently several blockchain networks. Bitcoin is probably the best known blockchain platform. Ethereum is another and as Bitcoin a cryptocurrency and permissionless platform. Stellar, Corda and Ripple are other payment platforms. Hyperledger Fabric is an enterprise permissioned blockchain for business transactions and has many of the features also required by DPKI. All these platforms are each supported by some kind of consortium with no relationship with Standard Development Organizations (SDOs) and none of the platform can be used as normative references and they are outside the jurisdiction of SDOs. DPKI cannot be based on an existing blockchain platform but must be self-standing specification, but it can make references to accepted concepts such as secure consensus protocols. An analysis of existing blockchain technologies has revealed that we need something quite different from the Bitcoin platform, but more like the capabilities of the Hyperledger-Fabric platform, especially as that platform has a concept of world state database. DPKI needs a DPKI directory holding updated certificate status information globally available to users of such information (by X.509 called relying parties).

Extension to current Public-key Infrastructure (PKI)

DPKI does not change the concept of PKI but allows interconnection of PKI domains by using the blockchain technology. At the same time, worldwide PKI information is made available locally at every node. PKI certificate and status information is forwarded to the blockchain to be validated by the node. If the certificates are successfully validated also by other nodes, they are made available at all nodes on the network through the replicated DPKI directory function. The information validation is done very thoroughly when PKI information is received from certification authorities (CAs), attribute authorities (AAs) and from adjacent nodes. Only genuine information is committed to the directory function of the ledger. Users (relying parties) that rely on the

information in public key and attribute certificates may interface to a node to retrieve PKI information from the DPKI directory function.

Use and migration of cryptographic algorithms

Cryptographic algorithms are use extensively both within PKI and within the blockchain technology. In PKI certificates are digitally signed by the issuer. In a public-key certificate, the public-key is used to verify digital signatures generated by the owner of the certificate. Use of cryptographic algorithms used for protecting communication protocols is made possible by PKI. Blockchains make extensively use of cryptographic algorithms for chaining block in the blockchain, for digital signatures on transaction to be able to identify origin. Also, the peer-to-peer protocol needs authentication integrity checking and possible encryption for confidentiality.

There can be several reasons for cryptographic algorithms to be replaced. Weaknesses may be found in cryptographic algorithms. A future threat from quantum computes may also require migration to post quantum cryptography (PQC). DPKI will from the beginning have cryptography migration capabilities.

How DPKI can shape the world

There are many potentially use of DPKI, i.e., requirements for interconnecting PKI domains to cover a wide area, e.g., the whole of Europe. Of potential uses are:

a) A Pan-European PKI by interconnection the national PKI domains to support the single market.

b) The World Health Organization (WHO) in its preparation for future pandemics wants to provide worldwide support for vaccination certificates. This requires PKI support and can only be obtained by a worldwide DPKI.

c) Support for international driver’s license.

d) Worldwide protection against telephone number spoofing.

e) Support for interconnection of European electricity networks.