CONSENT TOKEN

The first smart consent platform, sharing consent value between data subjects and data controllers

Green Paper

V.0.2

by Mindaugas Kiskis, Auste Kiskiene

April 2018

The purpose of this paper is to introduce the *Consent Token* concept and basic implementation proposals. This is not a White Paper (thorough project description) or a Yellow Paper (technical specification). These will be produced in the future if/when the project proceeds.

We welcome all constructive criticism and responses, we also invite interested Dev's / Contributors.

Join *Consent Token* Telegram / Discord to engage us!

See www.consentok.com for information and updates!

Executive summary

The need for consents is universal. In order to perform some operation with respect to the consenter, the interested party (data controller) must have a valid consent. For consenters granting consent is rarely exciting, the consenter does not participate in consent processing, there are no simple and easy ways to grant and cancel it. To address this, we propose a novel legal and technological approach – network consent and consent value sharing. Blockchain technology allows consent grants, cancellations and processing on a secure global network, eliminating the trust barrier between network members, and allows consent value growth and sharing among participating parties. Immediate practical application is possible in the field of ***privacy and personal data processing***.

Tokenized network consent – *Consent Token* – is a standardized smart contract-based consent, stored on a public blockchain, confirming a right to process personal data by the members of the *Consent Token Network*.

Introduction

Token in computer science is an object, which represents the right to perform some operation.

Consent in law and philosophy is a free unilateral act, which confirms someone's right to perform some operation with respect to the consenter.

Consent is a token in the fundamental sense. A token, which imparts certain obligations, not just provides entitlements. Thus, consent is a form of unilateral contract between the consenter and third parties (or the public).

The need for consents is universal. In order to perform some operation with respect to the consenter, the interested party (data controller) must have a valid consent. Consent may be granted (accepted), consent may be cancelled, and consent must be verifiable. Records are critical for lawful consent. In most multiparty and in all public contexts this requires some kind of systems for standardizing and processing consent(s). **The costs involved in the consent processing systems are substantial and imply economic value on the consent, regardless if the consent itself is granted (accepted) with or without consideration**. The value is significant in large scale multiparty consent context.

The consenter is usually an outsider to such systems. The consenter cannot influence the system beyond granting or cancelling consent. The consenter does not share any economic value of the consent, although it is acceptable that the user is compensated through certain set amounts (arbitrarily determined by the obtainer of the consent) for the costs (time and effort) involved.

We propose a novel legal and technological solution – network consent and consent value sharing. Blockchain technology allows consent grants, cancellations and processing on a secure global network, eliminating the trust barrier between network members, and allows consent value growth and sharing among participating parties. Network consent is consent grant to all members of the network. Network consent would be empowered by the consent value sharing – a fairer way to involve and compensate the consenter, while maintaining the freedom of the consent, and making the process of granting and maintaining consent exciting to the consenter.

These concepts may be implemented through *Consent Token* blockchain. Immediate applications may be for the field of ***privacy and personal data processing***, where consent is central, however the same concept may be useful for any field where individual consents are involved (for example, medicine).

Consent Token basic requirements and principles

In privacy and personal data protection, consent is essential for data processing and is the primary and most universal grounds for lawful personal data processing, for example see Art. 6.1(a) of the EU

General Data Protection Regulation (GDPR), and for legitimate sharing of customer data with third parties, see for example Recommended Practices on California Information-Sharing Disclosures and Privacy Policy Statements.

As it was noted, a consent imparts certain obligations on the consenter, and is a form of a unilateral contract, where the consenter voluntarily agrees that reasonably defined third party (or parties) perform some operation with respect to the consenter (consenter's private data in our case).

Consent needs to be **FREE**. Free means opt-in without external influence and not in exchange to any specific consideration. Consent shall not be condition of access to specific goods or services. *Consent Token* will comply with these conditions. The consenter will have to opt in and actively accept *Consent Token* terms and will be able to cancel the consent at any time by disposing of the *Consent Token*. For each consumer, the initial *Consent Token* will be issued free of charge and no specific remuneration will be offered to the consenter. The consenter by participating in the *Consent Token Network* would benefit from additional *Consent Tokens* (earned or acquired) and the sharing of the consent processing value, but not from the any goods or services to the consenter.

Consent Token will record consenter's **IDENTITY** (email, phone and other service/social-media account), which will need to be verified through existing services. *Consent Token* blockchain will not record more information than publicly shared by the consenter. Verification will be a precondition for blockchain record, not part of it.

Grant of consent may be realized by any means, as long as the will of the consenter is clear. Entering into a (smart) electronic contract, certified by retaining of the *Consent Tokens*, recorded in the public blockchain, is a legally acceptable form of consent creating **OBLIGATIONS** to the consenter. Main obligation will be agreeing to data processing by *Consent Token Network* participants.

Consent to the network (as opposed to a specific party) is not entirely legally new. Similar consents are found in many fields (e.g., donor consent in medicine or grant of consent to a group of companies). The clearly defined network membership is sufficient qualifying criteria for the consent to be specific. Content of the consent will be clearly presented to the consenter, when retaining the *Consent Token* and consent will be obtained from active consenter's acceptance (opt-in) of the *Consent Token* terms.

Consent Token in context

Landscape. Business personal data processing is essential for all modern business, regardless of the field. Business personal data processing is increasingly regulated and demanding. Many businesses try to implement complex consent obtaining and processing solutions, yet there are many actors, who process data without consent and without any knowledge of the data subject. Data brokers gather, process and

sell terabits of personal data about every person, who is not living off grid. Even if consents are retained, the consents are limited to a particular business, are conditional to the goods and services of a data controller, frequently exclude third parties, and may not be compliant with the legal requirements, for example of the GDPR.

On the other hand, data subjects have no simple and convenient means to issue consent. To obtain consent to process personal data, which is ought to be free and non-conditional on goods and services of the data controller, is notoriously difficult. However, consent is required for processing personal data in many jurisdictions. The GDPR, which enters into force on May 25, 2018, expands the data protection obligations of the companies and essentially requires novel qualified consents for most data processing activities. All businesses will need to maintain a comprehensive personal data processing documentation and have to review the existing consents of the data subjects (clients, users, employees, etc.) and ensure new rights of data subjects among other obligations. Solutions for these needs are lacking.

Majority of existing data protection related projects are focused on the anonymity and encryption. Few others are trying to find a way for the data subject to get directly paid for their personal data. For example, in some cases a person can get paid (insignificant sums, to be fair) if they answer survey questions or link their social media profiles to certain databases.

There are no projects, which would attempt to create easy to use, transparent and fair system of managing (granting/cancelling on the consenter side and obtaining/maintaining records on the business side) consents for personal data processing. Also, no projects allow consent value sharing.

Problems that need to be solved:

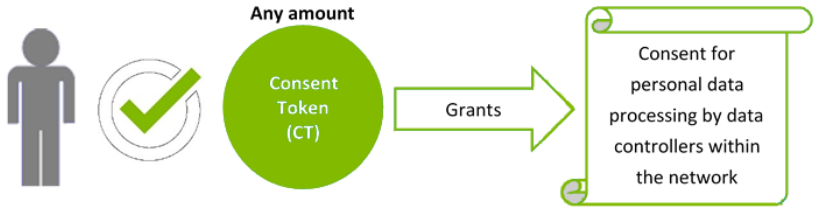
- Businesses need consent of the data subject;
- Shady actors process data without consent;
- Free consent is very difficult to obtain;
- Complicated consent recordkeeping (being able to verify the consenter's identity, existence of consent and validity thereof at any time);
- Consenter has to have free and easy way to cancel consent.

Proposed solution: tokenized network consent – *Consent Token* – standardized smart contract consent stored on a public blockchain, granting rights to process consenter's personal data to the members of the *Consent Token Network*.

Operating principles of the Consent Token

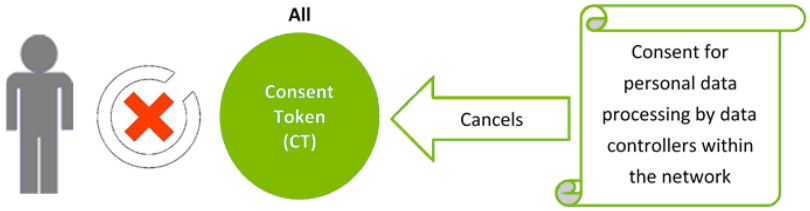
Data subject (individual) grants consent by accepting the *Consent Token* terms and obtaining *Consent Token(s)*.

Holding of the *Consent Token* confirms the consent to process his/her data by the data controllers in the *Consent Token Network*. The grant of consent, timestamp, identity of the consenter and content of the consent are recorded in the *Consent Token* blockchain, thus ensuring proper record and evidence of the consent.

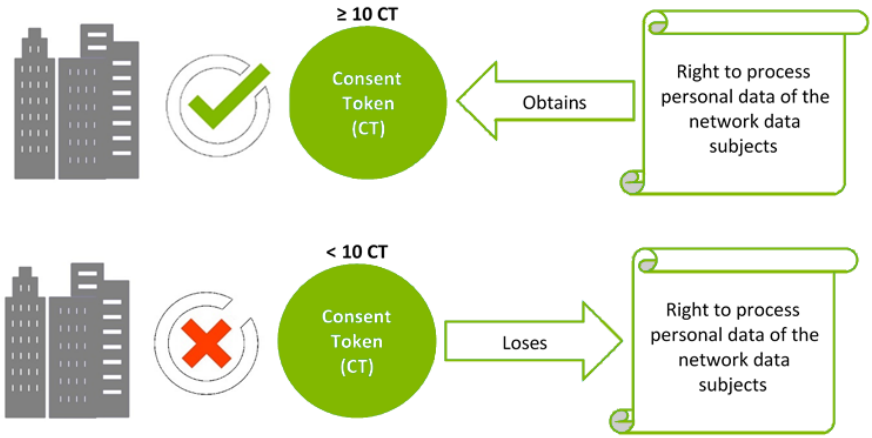


It is as easy to cancel consent, as to grant it.

Data subject (individual) cancels the consent by disposing of all the *Consent Token(s)* held. Disposal is effected either through market sale, or return of the *Consent Tokens* to the network. Consent is finally revoked within a set period of time, which is reasonably required to technically propagate and effect the cancellation through the network.



Data controller (business) obtains consents of the individuals in the *Consent Token Network* by obtaining *Consent Token(s)* on the market. Data controller loses the right to process personal data if it fails to retain a defined amount of *Consent Token(s).*



The data controller (business) by obtaining the *Consent Token* is entitled to process data of all individuals, who retain *Consent Tokens* at any given time. Consent is provided only for the data controller, who acquires *Consent Tokens* and is nontransferable. Consent does not allow transfer of data to any third parties, however such third parties may obtain the consent themselves by acquiring *Consent Tokens*.

Certain grace period for wrapping up data processing after the consent is cancelled (individual disposes of all the *Consent Tokens* held) may be established, and the cancellation will reset if the individual re-retains the *Consent Tokens*.

For all parties the consent is the same and the status of the consent is instantly verifiable in the public blockchain. Legal terms (content) of the consent are predefined in the *Consent Token* terms.

Consent Token does not affect existing consents, which data subjects have granted before obtaining the *Consent Token*.

Consent granted through the *Consent Token Network* is applicable to the legacy data, which is processed by the data controller, and due to regulatory changes (e.g. GDPR) can no longer be processed without consent. Thus, the *Consent Token* legitimizes processing of legacy data, which falls into the framework of the *Consent Token* terms.

Tiered consent terms (e.g. qualified consents) for holders of different amount of the *Consent Tokens* will be implemented. Thus, processing of certain data will be allowed for holders of higher amounts of the *Consent Tokens*.

Consent Token is not anonymous. Retaining of the *Consent Token* implies that user identity (email, phone, other basic identity info) are recorded in the blockchain. Identities of both individual and business participants will be public on the blockchain.

Consent Token blockchain is not a vehicle or a vessel for private data or for processing, it only grants the right to process data (including to collect it) in a legitimate way, for legitimate purposes and from legitimate sources.

Consent Token ensures that consent is freely given and is disassociated from any services or products provided to the individual consenters by the members of the *Consent Token Network*.

Scope of the *Consent Token* will be clearly limited in the *Consent Token* terms. Different scope (tiered consent) will be possible.

Consent Token special features, value sharing

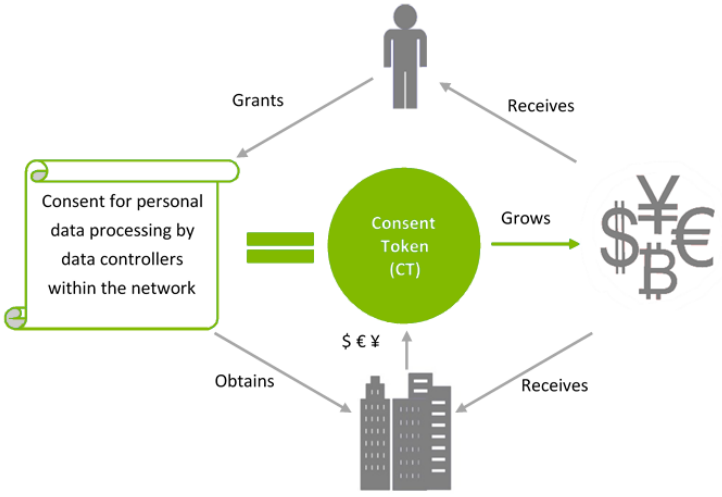
Consent Token is B2C focused smart contract. Obtaining and retaining of the *Consent Token* is a legal grant of consent and brings obligations on the consenter, thus it is different from many other blockchain tokens (especially cryptocurrencies) which provide entitlements only.

A predefined amount of *Consent Tokens* (at least one) may be obtained at any time free of charge by unique individual consenter (data subject) simply by accepting the *Consent Token* terms and registering for the *Consent Token*.

Additional *Consent Tokens* may also be purchased on a market or merited (Proof of Stake interest and Proof of Data consideration) by any individual consenter.

The data controller (business) may obtain *Consent Tokens* in the same way as individual consenters (including gaining additional *Consent Tokens* as an interest on *Consent Tokens* retained for a set period of time (Proof of Stake)) and have to retain them for as long as they wish to process personal data of the individuals, who retain *Consent Tokens*. Moreover, the data controller (business) has to retain a predefined amount of *Consent Tokens* (minimum of 10 (tentative), however larger set amounts or tiered amounts may be required by the *Consent Token* terms) in order to maintain the consents or expand the consents (in order to process some types of personal data).

By obtaining additional tokens either party will contribute to the costs of consent maintenance and will share the value of the consent processing, through appreciation of the *Consent Token*. Thus, all parties of the *Consent Token Network* share the value of the *Consent Token* and benefit from growth of the platform.



Rationale for holding the Consent Tokens

Consent Token demand will be warranted by universal need for data controllers (businesses) to obtain (renew) consents, easy entry into obtaining many consents at once (especially for new data controllers), and growth of data controller (business) ownership of the *Consent Tokens*.

Additional motivation will be efficiencies due to scale and centralization of the consent processing through *Consent Token Network*.

All parties will also benefit from the growth of the *Consent Token Network*. Appreciation of the *Consent Token* value would be expected from growth in demand for consents and network member growth.

For individual consenters the main benefits of obtaining and retaining the *Consent Token(s)* are:

- Simplicity of granting / cancelling consent for many data controllers at once.
- Sharing of value from consent processing.
- Extracting value by reselling the *Consent Tokens* (whether they exit the network or not).
- Earning additional *Consent Tokens*:
    - by retaining the *Consent Tokens* for a set period of time (Proof of Stake);
    - by submitting additional data to the paying parties (Proof of Data).

For data controllers the main benefits of obtaining and retaining the *Consent Token(s)* are:

- Simplicity of obtaining and maintaining consent from many data subjects at once;
- Low cost consent maintenance;
- Sharing of value from consent processing;
- Extracting value by reselling the *Consent Tokens* (whether they exit the network or not);
- Earning additional *Consent Tokens* by holding the *Consent Tokens* for a set period of time (Proof of Stake).

Consent Token blockchain

Obtaining and disposal of the *Consent Tokens* are recorded on the public blockchain. Holders of the *Consent Token* secure the public blockchain through well-known Proof of Stake methods.

Issuance, acceptance of the initial *Consent Tokens* will be made through the *Consent Token Network* organization. *Consent Token Network* will also offer initial *Consent Token* storage means (wallet) and block explorer.

Successive records to the *Consent Token* blockchain may be made through *Consent Token Network* service or other compatible services. *Consent Token* transactions record identity of the parties to the transaction.

Development. *Consent Token Network* organization will retain the predetermined amount of the *Consent Tokens* for development purposes. *Consent Tokens* issuance and initial allocation will be defined in the white paper, with account of the expert and community input.

Possible roadmap

The release of this Green Paper in April 2018 is intended to kick start the project. The goal of the Green Paper is to introduce the concept of the *Consent Token* to a wider public and interested parties: data controllers, data subjects (consumers), legal and business professionals, and blockchain developers. This Green Paper reflects years of experience in the privacy, data protection and knowledge management fields. Initial consultations with selected legal and business professionals, data controllers, and data subjects were also accounted for.

We are looking for constructive criticism and feedback. Tech developers and other contributors are also invited to express their interest in joining the development.

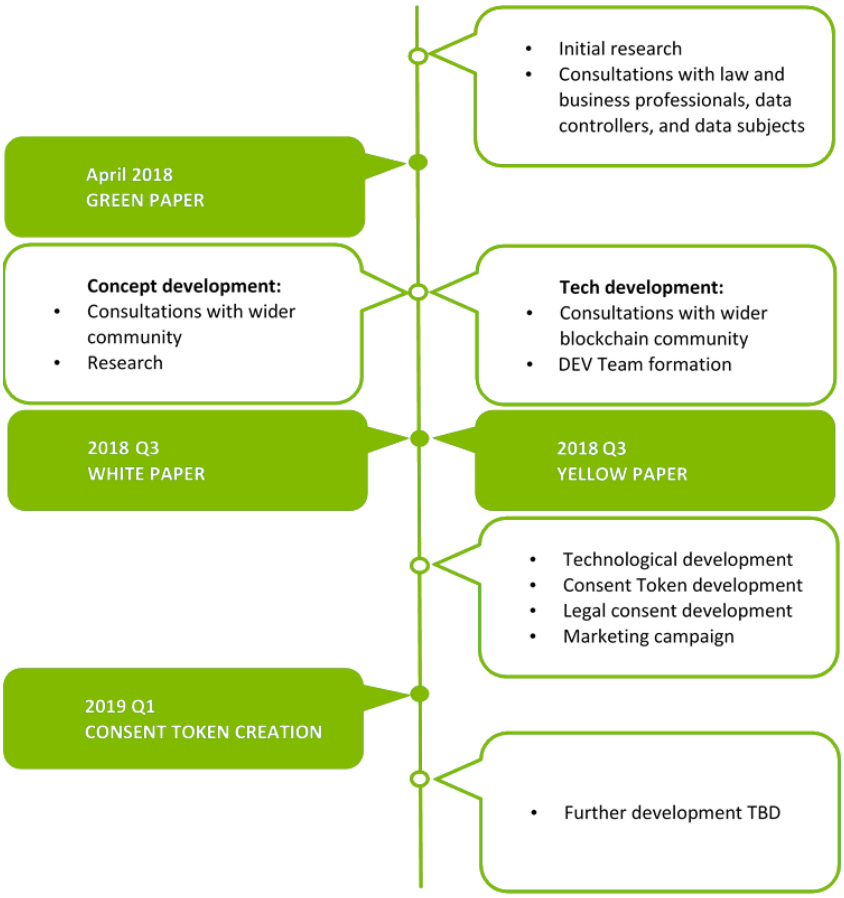
Consent Token will proceed with the concept development, tech development, legal consent development, and marketing of the project.

The concept development shall test the initial *Consent Token* idea, research practical applications of the *Consent Token*, develop consent management model and explore other connected innovations (for example, tiered consent development and "proof of data" method for earning *Consent Tokens*). Consultations with the community (data subjects), and a focus group of data controllers will be part of this phase.

Concept and tech development will first result in the White Paper and the Yellow Paper respectively with detailed implementation road map. Tech development will follow up with software development and then test-net public release.

Due to regulatory differences, during the initial period *Consent Token* will only be available to the EU and the US residents (as determined through id (phone) verification).

Preliminary roadmap for the project:



Discussion (open questions)

- ***Content of the Consent Token consent***. Will be proposed for public discussion in Q2 2018.
- ***Tiered consents*.** The idea is to require larger *Consent Token* holdings for data controllers, who want to process more extensive data for various purposes. The proposal is open to public input.
- ***Undesirable data controllers*.** Consent or no consent does not prevent each of us from abuses, such as Cambridge Analytica. Many excessive and unethical data processing activities will be expressly disallowed in the consent development process. This issue may also be partially addressed through tiered consent, by pricing-out the undesirable activities. This would at least allow network members to benefit, if the data controller is determined.
- **Decisions on removal of certain participants from the network**. Network will remove participants, who operate in violation of the network principles and rules. Consensus decisions on removal may also be possible for arbitrary causes (such as certain undesirable data controllers).
- **Public access to and transparency of the Consent Token blockchain**. Does it have to be fully transparent and accessible to anyone? Or just to holders of the *Consent Token*? Or organized in

another way (e.g. individual consenters can see business ids, but not other consenters; businesses can see individual consenter's but not other businesses).

- One possible useful side effect of the *Consent Token*, even for non-members of the *Consent Token Network*, would be ***free market-based appraisal of damages in cases of data breaches***.

About the authors

Prof. Mindaugas Kiskis

Mindaugas Kiskis is the Law and Management Professor, privacy attorney, technology geek and entrepreneur.

Prof. Kiskis has more than 20 years of hands on experience in the fields of Privacy and Data Protection, Intellectual Property, Technological Entrepreneurship. Mindaugas has been advising international and local businesses, including many blue-chip companies, in the EU and the US on data protection and privacy matters. He has also cofounded three technological ventures and is specialized in the regulatory and management issues of technological and innovative enterprise, legal trailblazing and setting new precedent.

Mindaugas works globally. He has worked in the US (2017-2018), China (2013), Canada (2011). He was the Fulbright fellowship at the Arizona State University (2007-2008), Markle fellow at the Oxford University (2003).

Dr. Auste Kiskiene

Auste Kiskiene is an entrepreneur, manager and Management and Entrepreneurship Professor.

Auste has more than 15 years of experience in business and project management. She has been a cofounder and COO of entertainment, education and technology startups (first in 2001 – events and advertising agency). Auste has experience in R&D and innovation management, technology and market analysis, information and knowledge management, quality control and management, strategic management and policy setting.

Auste currently is a Fulbright Visiting Scholar at the Montana State University (USA, 2017-2018) and a Visiting Professor at the Tongji University (Shanghai, China).