GENERAL MEETING PROXY VOTING ON DISTRIBUTED LEDGER

Product Requirements v1.4

June 2017

NATIONAL SETTLEMENT DEPOSITORY
MOSCOW EXCHANGE GROUP

strate
always discovering

Nasdaq

dcv

SIX Securities Services

OVERVIEW

This document was prepared by the CSD Working Group on DLT in collaboration with SWIFT to define the product requirements for the e-voting solution based on Distributed Ledger Technology (DLT) shared by CSDs operating in different and diverse markets.

The members of the CSD Working Group on DLT are:

- NSD (Russia)
- Strate (South Africa)
- SIX Securities Services (Switzerland)
- Nasdaq (Nordic)
- DCV (Chile)

This document is written with several premises in mind, in which all members of the working group firmly believe:

Distributed ledger foundation. Modern DLT platforms provide provable transparency and finality and mitigate risks much better than traditional messaging-based solutions, enabling business benefits not possible with current systems.

Locally applicable solution. Our solution aims to offer enough flexibility so that it can be implemented independently on most local markets without compromising its potential for global integration. Each local solution must be able to define its own architecture and details of operation if it follows the general common principles.

Focus on the global context. DLT solutions offer maximum value when they are used by all involved parties, locally and cross-border. Our solution emphasizes requirements shared by participant markets, so that cross-border integration of local systems compliant with these requirements does not compromise the integrity of the distributed ledger.

Alignment with market standards. DLT solutions are currently a novelty in the industry and the key concern for adopting organizations is to ensure smooth transition in both technological interoperability and the understanding of the processes and terms by the stakeholders. Our solution is aligned with the existing industry standards like ISO20022 on both technical and conceptual levels.

CONTENTS

1. INTRODUCTION

1.1 Target Audience

The working group expects that this document will be useful for the following groups of people:

- Product managers, architects and analysts in charge of corporate actions and general meeting voting solutions;
- Innovation managers and architects, looking for well-defined DLT use-cases and requirements;
- Standards managers and experts, looking to develop ways to standardize and integrate DLT-based solutions.

We assume that the reader is familiar with the general meeting processes and has a basic understanding of DLT.

1.2 Problem Statement

Voting at general shareholder meetings is a process that involves many parties and is subject to numerous risks. The administrator of the meeting must ensure that all voting rights are issued correctly, are delivered to securely authenticated shareholders or their authorized proxies and the votes are counted and reported correctly. In many countries this process has been made partially digitized, but that does not eliminate many of these risks.

The most prominent problems today are complexity of the processes involved in the voting and lack of finality.

For major shareholders it is important that the voting process is streamlined and transparent, the meeting results are reported precisely, quickly and with guaranteed finality, so that they can rely on these results in a legally binding way.

For minority shareholders the problem is that they typically have to go through complicated process to exercise their voting rights – there is no common and easy way in all markets to vote or assign a reliable and controlled proxy. The value of voting can be small for them. However smooth, easily accessible and reliable voting process may encourage them to vote. Lack of a good predictable system prevents them from doing it, reducing the turnout at the general meeting.

For foreign shareholders the complexity rises to a much higher level. Expectations of means of authentication, understanding the process and relevant laws and local practices are high. In some cases the interface language may also prove to be a barrier to vote. These shareholders would like to be able to exercise voting rights on their foreign investments just as easily as they do locally. However, this is not always achieved with current voting mechanisms.

1.3 Objective

This document aims to provide a set of requirements encompassing all major needs of voting on general shareholder meetings, addressing problems present in the current voting systems. These requirements are designed to be independent of any market as much as possible and are extensible, supporting further customization.

1.4 Document Structure

This document contains a set of common requirements, as discussed and agreed by the members of the CSD Working Group on DLT.

The structure of the document is as follows:

Chapter 2 describes functional requirements, defining the actors, the voting process and its various high-level details, including both generic minimal viable product (MVP) and various local extensions.

Chapter 3 describes trust requirements to the DLT solution designed to mitigate the risks of the e-proxy voting process incurred in the traditional systems.

Chapter 4 describes data entities necessary to support the process that must be stored on DLT to fulfill the trust requirements.

Chapter 5 describes non-functional requirements of the software solution.

Chapter 6 describes the plans for future development of this document and the e-proxy voting on DLT problem in general.

1.5 Alignment with the Industry Standards

The financial industry has business standards for messaging and data that enable the creation of robust, interoperable multi-party business processes by reducing the

ambiguity of specifications and fostering efficient re-use of knowledge, skills and technology. There are two ways in which these standards work.

First, standards specify a methodology to capture and publish formal business specifications in a consistent and precise way.

Second, they provide governance processes that can be used to standardize the content and evolution of the business specifications themselves. These processes are among the key benefits of reusing the existing standard definitions for the DLT implementations.

The benefits of reusing existing standards are twofold:

- Avoiding ‘re-inventing the wheel’ in terms of business definitions;
- Facilitating interoperability amongst DLT implementations and with existing financial industry infrastructure including electronic messaging.

These benefits can be considered as ‘quick wins’ that can accelerate the implementation and acceptance of DLT technology for industrial solutions while the work on producing full, all-encompassing specialized DLT standards is underway.

The requirements in this document are aligned on a high-level with the business layer of the ISO20022 standard.

1.6 Out of Scope

There are notable topics which are not covered in this document. Among them are the technological architecture of the solution and the integration methodology between systems built according to these requirements.

The architecture of the solution is something that we believe should be independent of the high-level standard. Architecture is a specific detail of implementation and can differ from one solution to another even if they operate within the same legislation. Organizations implementing these requirements will use their own judgment to design the most efficient architecture for their solutions.

In addition, the architecture will be built around or will even impose some local features on the solution. The working group would like to make it possible to customize each local system as required by its administrators, so we do not define any concrete architecture in the product requirements and leave it as an implementation choice.

The integration methodology may be added to a future version of this document. The working group sees the global context as a key opportunity in this effort, and shared

common requirements are the first step towards defining a methodology for DLT standardization.

2. FUNCTIONAL REQUIREMENTS

Functional requirements describe what the system must be able to do and how it should be accomplished. Functional requirements are driven by the needs of the business and the market, regulators' requirements and local laws.

This chapter contains a high-level set of requirements necessary to describe an MVP for an e-proxy voting system. The requirements also outline a set of extension requirements that cover the specific needs of the markets in Russia, South Africa, Switzerland, Chile, Nordic countries and Baltic countries. We believe that these requirements will also cover many other markets with limited adaptations.

2.1 Functional Role Definitions

Functional role definitions describe the actors who have rights to process transactions on the distributed ledger.

There are three actors in the system. Their definitions are synchronized with the e-proxy voting ISO20022 messaging standard.

Issuer or Issuer Agent. The legal entity that has the right to issue securities or the organization appointed by the issuer for the purposes of administration of a security issue or processing of a corporate action or a meeting event. In some cases, the issuer acts as its own agent.

Intermediary. Institutions providing services to other institutions in the frame of the proxy voting processing chain, i.e. a proxy voting agent.

Voting Party. A party that has the right to vote on resolutions and agenda items on a shareholder meeting.

Auditor. An actor who does not take actions that impact the business process, but may have privileged access rights that allow it to verify that certain parts of the process are executed correctly.

2.2 Process Flow

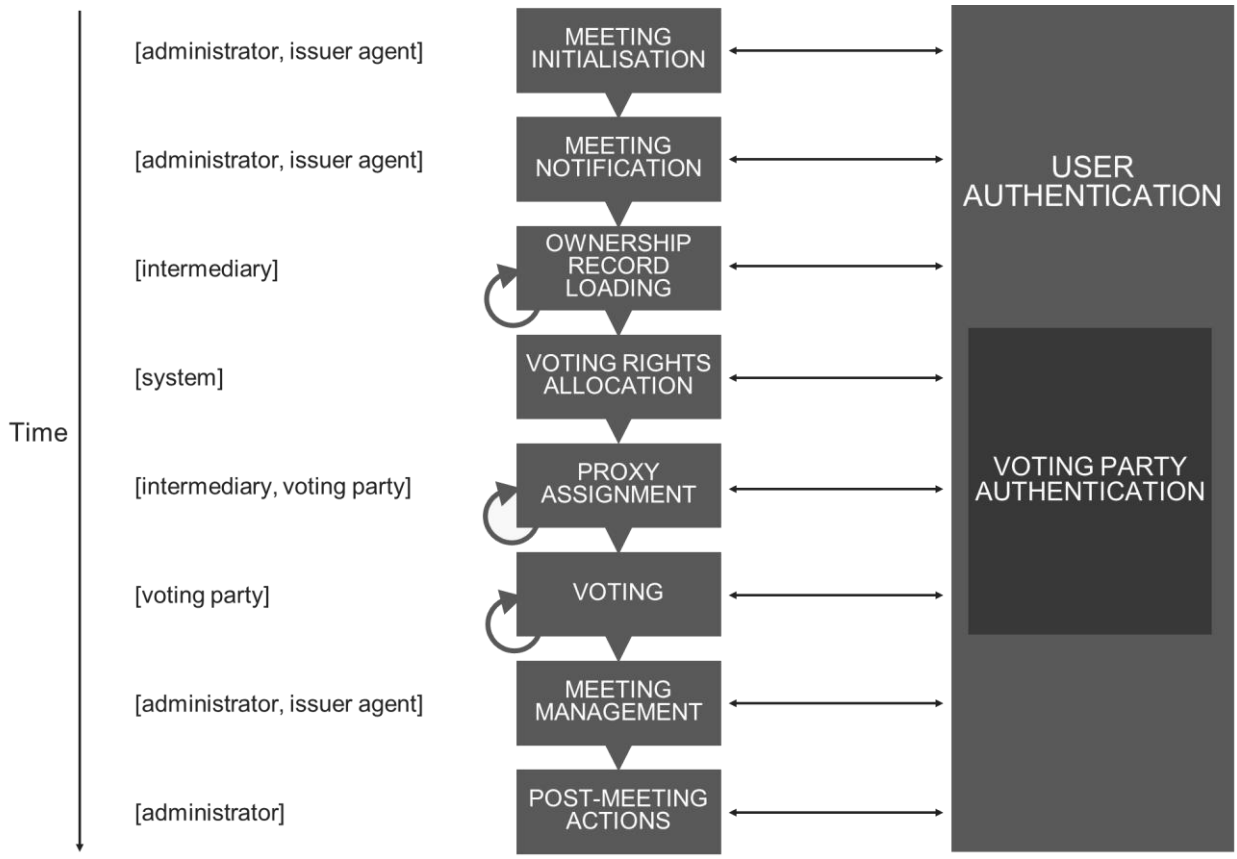
E-proxy voting process involves multiple steps that in general are similar between different countries. Depending on the local regulations they may be extended or placed

in different order, but it does not disrupt the general picture or change functional requirements, which can be mapped to the steps regardless of the order of these steps.

Each step aims to accomplish a certain objective in the process. These objectives usually result in some transactions being performed between the actors. We have analyzed whether these transactions generally occur on the distributed ledger (and benefit from the trust enabled by it) or can be recorded independently in traditional systems.

#	Step	Description	Data records
1	Meeting Initialization	Capturing of agenda and setting of timelines (meeting date and record date).	On blockchain
2	Meeting Notification	Informing registered owners of the meeting dates and agenda.	Off blockchain
3	Ownership Record Loading	Loading list of owners and ownership records at the voting record date into the blockchain.	On blockchain
4	Voting Right Allocation	Issuing of tokenized voting rights to all Voting Parties who are eligible for voting.	On blockchain
5	Voting Party Authentication	Authentication of the user able to vote via one of the means supported by the system.	Off blockchain
6	Proxy Assignment	Transfer of voting rights from the initial owner to another party.	On blockchain
7	Voting	Issuing voting instructions by the Voting Parties using their tokenized voting rights.	On blockchain
8	Meeting Management	Live streaming of the general meeting online, chat facilities and various services, including running and closing the meeting and processing and distributing the results.	On and off blockchain
9	Post-meeting actions	Any events that happen after the meeting independently of the rest.	Off blockchain

These process steps are also depicted on the figure below:



2.3 Minimal Viable Product Requirements

The goal of creating common requirements was to reconcile them, without creating a conflict between shared and market specific requirements. Within the scope of this document MVP requirements accomplish this goal. They encompass all shared parts of the process that are present in the majority of reviewed countries. The system built according to the MVP requirements would not necessarily correspond to any existing market, but could be easily extended to match the requirements of a specific market.

It is our expectation that this set of MVP requirements represents a globally shared view of how the core of the e-proxy voting business could look like and that it could be used anywhere to guide the implementation of a new DLT-based solution for e-proxy voting.

The MVP requirements are structured according to the steps of the process that they relate to.

2.3.1 Meeting Initialization

Requirement №10: The Issuer Agent is able to publish and update the meeting agenda and supplementary materials. Voting Parties are able to view the published meeting agenda and receive notifications about it.

The meeting agenda can contain preliminary or a final list of topics (with voting options) that will be discussed at the meeting. The purpose of storing them on the blockchain is to ensure their immutability and legal significance, as well as to provide proof of their publication. Any supplementary materials may also be made available, and may be stored directly on the distributed ledger or externally. Providing the actual notification service (reaching out to the potential voters for the first time) is a value-added service that may be implemented outside of the system.

Requirement №150: The system must support statutory and cumulative voting types.

The two most common types of voting are statutory and cumulative voting. In statutory voting the holder of each voting right is eligible to cast a vote for one of the mutually exclusive options, with the option with the majority of votes winning. In cumulative voting, votes may be cast for multiple options, as stipulated, with several options where the option receiving most votes wins. This form of voting is most commonly used for selecting the members of the Board of Directors.

2.3.2 Ownership Record Loading

Requirement №40: The Intermediary is able to load the list of all potential Voting Parties to the distributed ledger.

The Intermediary holds shares in the accounts opened in the names of beneficial owners or other Intermediaries. It can identify all potential Voting Parties eligible for the meeting based on local rules. The list of Voting Parties is then used to provide them with access to the meeting agenda and actions related to voting. In some cases, due to local legislation, it is possible that the Voting Party is not the beneficial owner even before any proxies are assigned.

Requirement №50: The Intermediaries in the custody chain are able to load the list of all potential Voting Parties to the distributed ledger even if each one of them individually can't achieve that. The custody chain supports propagation of the necessary data up and down the chain.

In most countries the Intermediaries are also able to hold nominee accounts with the registrar, the central securities depository or with other Intermediaries. In this structure

registrar or CSD may not know the beneficial owners as they hold their personal accounts with the Intermediaries through nominee accounts. The chain of Intermediaries can be long and each Intermediary can be responsible for loading only the lists of Voting Parties who hold accounts directly with them and can forward the rest of the responsibility to the next level Intermediary for further processing of Voting Parties. The exact mechanism of propagating the data through the custody chain may vary depending on the participating actors, their service agreements and the local specifics.

2.3.3 Voting Right Allocation

Requirement №80: It is possible for the beneficial owner to decide if he wants to participate in the voting process.

Beneficial owners may not be interested in participation in the voting process. The system must provide a mechanism for them to control their participation. It can be implemented in any number of ways that correspond with the local features - mandatory opt-in registration, deferring voting rights to their custodian by default and opt-in override, participation by default with voluntary opt-out, or any other as required by local legislations.

Requirement №120: An Intermediary is able to assign tokenized voting rights to Voting Parties according to their ownership records in compliance with the Issuer rules and local regulations.

The amount of issued voting right tokens is dependent on many things, possibly including record date cutoff, share blocking, voting restrictions, re-registration and so on. The information required to calculate voting rights is known by the Intermediary who holds the account of the beneficial owner. The Intermediary must apply all restrictions to the position of the beneficial owner and issue the voting rights on the ledger accordingly.

Requirement №121: The system supports calculation of Voting Rights according to the position dates. The most recent position up to a set record date is taken.

Record date is a practice that is used in most countries. It is used as a cutoff date from which any changes to positions no longer affect the voting rights. Positions prior to the record date can still be used in pre-voting (if it is allowed), but will be readjusted according to positions at the record date.

Requirement №122: The system supports calculation of voting rights using different share types. The share types can be defined at the time of the initialization of the meeting, along with the rules according to which they are allowed to vote. The system supports a coefficient rule (amount of voting rights = coefficient x position).

Companies often issue shares of different types (typically common and preferential), which may have different voting rights assigned to them - e.g. preferential shares may not be allowed to vote on certain questions. The rules are set at the time of initialization of the meeting and must be processed by the system, making their application transparent to the Voting Parties.

Requirement №124: The system supports reconciliation of the holding records between all Intermediaries and the Issuer Agent so that a single reconciled source is used on all segregation levels for determining Voting Rights.

The custody chain includes many Intermediaries, each having its own records of holding. This ledger can be reconciled only with the holdings records at intermediary level at CSD/registrar/issuer. A reconciliation algorithm between different records must be implemented by any implementation of the system to solve this problem. The exact specification of that algorithm may be determined by a local implementation.

2.3.4 Voting Party Authentication

Requirement №60: An Intermediary is able to securely authenticate all eligible Voting Parties who hold accounts at it.

The Intermediary provides Voting Parties with the access to perform various actions to the shares that they hold accounts with. Performing these actions requires secure authentication of the Voting Party. This authentication can be done in any way that is convenient to the Voting Party and the Intermediary - offline using government-issued IDs or online via the identification system of the Intermediary on any device that it supports.

Requirement №61: The authentication means provided by the system must be non-discriminatory and equivalently valid for all purposes.

It is likely that any implementation of the system will support multiple means of authentication. It is important that any secure authentication method is supported in full to avoid discrimination towards certain groups of voters.

Requirement №62: The proof of authentication must be stored on the blockchain, and the personal data that the proof points to must be safely stored by the Intermediary to allow access only to those who are authorized to read it.

The authentication process happens outside the blockchain, but it is important that the blockchain wallets contain proof that they have been given out to the correctly authenticated person. The personal data may not be stored on the blockchain due to data privacy laws in many countries, but it can be stored in a traditional system hosted by the Intermediary. It would be the responsibility of the Intermediary to properly authorize access to this data.

2.3.5 Proxy Assignment

Requirement №90: A beneficial owner may assign a proxy to act on his behalf with regards to offering meeting agenda items and/or issuing voting instructions. The act of assigning a proxy must be recorded in the blockchain.

Beneficial owners often do not want to participate personally in the meetings or voting and opt to delegate that responsibility to another trusted party. They may provide that party with explicit instructions on how to vote or may just instruct to use its own judgment. The proxy can be an individually appointed manager representing the beneficial owner, a custodian acting in the interests of its clients or some other party.

2.3.6 Voting

Requirement №159: A Voting Party is able to cast voting instructions according to its voting rights.

Voting may happen either during the meeting time itself, any time between the record date and the end of the meeting, or even prior to the record date ("pre-voting"), depending on what the local rules allow. A Voting Party may issue voting instructions by using its voting right tokens.

2.3.7 Meeting Management

Requirement №160: A Voting Party is able to see how it cast its voting instructions and that its voting instructions are included in the vote count.

It is not enough for the Voting Party to anonymously cast a voting instruction. Often the Voting Instructions may be rejected, adjusted or not processed for various reasons. The

Voting Party must be able to see that the cast votes have been properly used and counted in on the outcome of the voting.

Requirement №165: The voting campaign and the meeting can be closed by either the Issuer Agent or automatically by the system process according to the pre-set rules.

Closing the meeting is an important cutoff point in the process that prevents further instructions to be issued and allows the results to be calculated. The closing time acts as a point in the process from which finality (in business sense) can be achieved.

Requirement №170: All actors are able to calculate the outcome of the voting campaign once it has finished.

It must be possible to independently verify the results of the voting process. The distributed ledger must contain proof that the result has not been tampered with and that all actions are traceable to their origin. This verification must respect various confidentiality requirements of the system. The DLT technology itself provides most of the functionality to satisfy this requirement.

2.3.8 Post-meeting actions

Requirement №220: It is not possible for Voting Parties to see or deduce the identities of the beneficial owners (or proxies) using the system. All actors may only see that voting rights have been allocated, but only the Voting Party who owns them may see how many voting rights it has. Only the Voting Party who has cast a voting instruction is able to see its effect on the voting process.

Anonymity of the beneficial owners and confidentiality of their actions is important to both them and the regulators. If the identities behind the Voting Parties are exposed, they may become subject to pressure by other interested parties so that they vote in a way that may not serve their best interest. The system must conform to the information security practices of handling personal data in a way that the identity of the beneficial owners cannot be deduced using the analysis of the data that is openly available.

Requirement №221: It is possible for the Voting Party to disclose some of its private information to parties that require it by the process. This information may be disclosed either voluntarily or if the process demands it.

Anonymity is typically required to protect private data against other voters, but it may be necessary (by law or otherwise) to disclose some of the private information to certain parties (e.g. auditors or the issuer) for the voting process to work legitimately. The

system must support this functionality in a way that allows the process to function, but does not compromise the privacy of the Voting Parties.

Requirement №230: There exists an Auditor role with the elevated access rights to the blockchain. The Auditor can review the data with limited access. It must be possible to assign the Auditor role to multiple independent trusted parties.

The financial industry is heavily regulated in all jurisdictions and the regulator requires access to a lot of confidential information. The system must be able to provide access for the regulator and auditors to that information to simplify and reduce the cost of many compliance processes.

2.4 Extensions Requirements

Alongside the MVP, we have listed a set of additional requirements that could be used to extend the system. A local implementation may add any or all of them. This list is not exhaustive or complete, but allows the markets of Russia, South Africa, Switzerland, Chile, Nordic countries and Baltic countries, and possibly others, to be serviced.

The extension requirements are presented in the same way as MVP requirements, but are structured according to the functional area that they modify, rather than by the process step. It is possible that a single set of extensions affects actions in multiple process steps.

2.4.1 Agenda Management

Requirement №11: The supplementary material can be attached to the meeting agenda and viewed through the system. The supplementary material itself is not stored on the distributed ledger.

The supplementary material can contain financial statements, reports and any other media that may be of interest to the shareholders prior to or after the meeting. The supplementary material can be of significant size and should not be stored on the distributed ledger by default, but the ledger can provide access links and/or verification hashes to it. The implementation of the actual storage of these materials can be decided individually by each service provider.

Requirement №20: A Voting Party is able to propose meeting agenda items to the Issuer Agent.

In many cases, the meeting agenda is formed before it is published and does not change afterwards. In some cases, however, a process for proposing new agenda items is required. This may be necessary, for example, when new agenda items are proposed during the actual meeting.

Requirement №30: The Issuer Agent is able to accept or reject the proposed meeting agenda items.

When shareholders propose new agenda items, processing them is dependent on legislation or rules of a particular organization. It is necessary for the Issuer Agent to be able to enforce these rules. It can be implemented in various ways, including encoding the rules directly into the system or allowing the administrator to explicitly accept or reject proposals.

2.4.2 Meeting Notification

Requirement №12: The system is able to perform the initial notification of all potential Voting Parties.

It is important that all potential voters are notified of the meeting details in advance. Reaching all of them can be very difficult and is a process of its own, but a simple feature of using standard contact details (email or SMS) can be implemented by the proxy voting system. This capability will not be built on blockchain, although its use can be triggered by the initialization of the meeting on the blockchain.

2.4.3 Electronic Identification

Requirement №70: The system is able to securely authenticate beneficial owners (or their Proxies) via electronic identification (eID).

In some countries, the government or government-sanctioned organizations issue electronic forms of ID. These eIDs can be used to securely authenticate their owner in secure manner. For the Voting Parties who own these eIDs, using them is often the preferred way of authentication and it must be supported by the system.

2.4.4 Proxy Chains

Requirement №100: It is possible for a proxy to assign further proxies to act on its behalf. The act of assigning a proxy must be recorded in the blockchain.

In some cases according to local legislations the beneficial owner may not possess the right to vote as well, which can be assigned to its Intermediary by default. Intermediary can re-assign voting rights to the beneficial owner as a proxy for its own shares to be able to vote personally. The beneficial owner can, in turn, delegate further to an actual proxy, forming a chain of proxies.

2.4.5 Automatic Custodian Proxies

Requirement №110: It is possible for an Intermediary to assume a proxy role on behalf of beneficial owners who hold accounts at it automatically unless the beneficial owner expresses a desire to participate in the voting directly.

In some cases it may be beneficial for proxy rights to be assigned to the Intermediary automatically, requiring the beneficial owner to explicitly express the desire to participate in the voting. This may be desirable for the retail shareholders who hold limited voting rights to make any difference. Intermediaries may pool their voting rights together and vote in the interest of all of their beneficial owner clients. This is subject to any rights granted to the beneficial owners by local legislation or rules.

2.4.6 Voting Right Responsibilities

Requirement №123: The system supports re-registration and correctly determines which shares are eligible to vote.

In some countries, the custody chain cannot participate in the voting in the normal way. It may require that all shares that intend to participate in the voting are de-registered from their custodian and re-registered at the registrar or another designated entity such as the repository.

Requirement №125: The system supports sending external notifications that the Voting Rights have been issued.

It may be necessary for external systems to know that the voting rights have been issued. In different countries it can be used for different purposes: issuing offline certificates of attendance, blocking shares to prevent their trading until the voting is over or for another reason.

2.4.7 Ownership Record Updates

Requirement №130: An Intermediary is able to reload ownership records of a Voting Party. The system is able to recalculate the voting right tokens according to the updated records.

Some laws require the updating of the initially loaded voting rights with the new positions. This may occur due to trading (when it is permitted), reconciliation settlements, mistakes in applying rules or legislation and so on. The frequency and detailed requirements of the updates are unique to each jurisdiction.

Requirement №131: The system must support pre-voting, issuing voting rights and casting votes prior to the record date.

In some countries it is possible to vote early, prior to the record date. The votes can be cast early and are adjusted later if there are any changes in share ownership at the registry or depository.

Requirement №132: When ownership records are updated, the system supports validation of already cast votes and can adjust them if it is necessary to keep the counts consistent.

Position updates affect voting rights, which in some cases (pre-voting or corrections) can be already cast. The system must keep itself consistent at all times, so if voting rights amounts are updated, cast votes may also need to be adjusted. The exact algorithm for adjustment of cast votes can be defined by each implementation.

2.4.8 General Meeting Services

Requirement №155: The system must record the events that happen at the physical meeting and store them on the distributed ledger according to local legislation or company requirements.

Physical meetings have additional requirements to the record-keeping compared to digital voting. In most countries it is required that the voters pre-register, that the protocol is properly recorded etc. Recording this information in the blockchain alongside the data required for digital voting will increase the transparency of the process.

Requirement №156: The system must provide services to the users voting electronically during the meeting, including the video streaming of the physical meeting.

Users who vote electronically benefit from the convenience and ease of voting, but pay for it by being absent at the meeting and missing out on the potentially important

discussions that happen there. The system would add a lot of value to the whole process if it could increase the involvement of the online voters by providing them with more means to take part in the meeting, e.g. access the video stream, being able to ask questions, etc.

Requirement №171: The Issuer Agent is able to publish meeting minutes and results on the distributed ledger.

In most jurisdictions, Issuers are obliged to provide specific reports on the general meeting results and minutes. If these reports were stored in the blockchain, they would benefit from its access control and immutability, thus enhancing their legal standing.

2.4.9 Review Voting in Progress

Requirement №180: Certain actors are able to calculate the status of the voting campaign when it is in progress and only some of the votes have been cast.

Voting is normally done blindly, with the Voting Parties not being able to see the progress until the results are out. But for the Issuer Agents (e.g. issuers or registrars), regulators or auditors it may be necessary to see the progress.

2.4.10 Administrative Adjustments

Requirement №190: The Issuer Agent is able to adjust the vote amounts.

In some jurisdictions, legislation and other rules may cause adjustments to votes issued by the Voting Parties. The Issuer Agent should be able to detect the instructions liable for adjustments and execute the adjustments. It is only possible to adjust the amount of votes, not the selected outcome. This function must be designed in a way that doesn't give the administrator possibility to misuse it.

Requirement №200: The Voting Party is able to see how its votes have been adjusted by the Issuer Agent.

The mechanism for adjusting the votes must be transparent. Voting Parties whose votes were adjusted must be able to easily detect and review the adjustments with any additional information (e.g. reasoning behind them). This information must be stored on the blockchain so that it can hold weight in the courts should the Voting Party decide to challenge the adjustment.

3. TRUST REQUIREMENTS

The main added value of DLT is that it enables trust in trustless environments. In traditional systems, trust is typically achieved by designing business processes in a way that create incentives for parties to act with integrity and prudence. These processes come with a lot of double-checking, audit, reconciliation and other validation and correction mechanisms necessary to make the process work. These steps create a significant overhead in otherwise simple business processes.

DLT-based systems take another approach to trust. DLT technically guarantees that the rules of the process are the same for every participant and that these rules are followed. It eliminates the need to trust actors in the transactions – the trust is now placed in the system itself.

At the same time DLT also plays a role of an immutable golden copy of all data – so that no peer-to-peer reconciliation is needed, as the correct data is always stored in the blockchain.

These two properties together are the foundation which can drastically decrease the overhead in many typical processes in the finance industry, allowing for a much higher level of service that was not possible before.

The lack of trust essentially means that there are risks that have not been mitigated to an acceptable degree. These risks are inherent in the traditional systems. This section elaborates on the risks specific to the e-proxy voting process and discusses how they can be mitigated via a DLT solution.

3.1 Disruption of the business process

Risk	Description	Mitigation
Incorrect vote counting or reconciliation.	Certain processes that happen outside of voting (e.g. securities lending), inherent in the voting process (e.g. pre-voting), or resulting from malicious intent of one of actors may result in incorrect counts of votes and incorrect voting outcomes.	Voting rights are represented by special tokens in the blockchain. The tokens are created strictly according to the legislation at the authorized node using relevant position information.

Risk	Description	Mitigation
Exclusion of participants from voting	Cut-off dates are present in many countries. Asset movements around these dates are not always recorded on time or correctly, potentially affecting not just vote counts, but also shareholder eligibility for participation in the meetings.	Voting rights tokens are generated at the source which has the most up-to-date information. The blockchain code automatically ensures voter eligibility and forces all other nodes to reconcile with the source if they have conflicting data.
Disruption of the process by a malfunctioning, malicious or compromised actor, performing actions within the rights assigned to that actor.	The business process supported by the system must be thoroughly tested and verified to prevent situations where a node, behaving legally as defined by the system, can cause unwanted consequences resulting in some sort of system disruption.	The blockchain code strictly defines the eligible actions at any state of the system. It can be formally verified that any valid action always switches the system to a valid state.
Incorrect initial loading of data	Regardless of how well-protected the data is on the distributed ledger, it is possible for it to be incorrect before it is entered into the ledger. This can affect anything in the system, from generating minor errors to completely disrupting the process.	Most error-prone data items (e.g. positions) are entered via multiple channels and the system has a built-in reconciliation mechanism that will highlight problems.
Disruption of the process by altering the code that governs restrictions and process.	The codified business process defines the rules by which all process participants must abide. If this process is changed in a way that some of the participants expect, their actions will have different meaning than they intended and may render the system completely inoperable.	Modification of the chain code and/or smart contracts, which govern all processes and restrictions in the blockchain, is only possible by a consensus of a sufficient number of nodes. Depending on the system architecture, it may be possible to not allow any changes for anyone for any reason. In case changes are allowed, they can also be

Risk	Description	Mitigation
		governed by a change process, which would prevent undesirable changes from happening.

3.2 Tampering with data

Risk	Description	Mitigation
Tampering with any voter data in the distributed ledger: voting rights, instructions or final vote counts.	Tampering with data may alter the results of the voting or mislead the stakeholders.	All data in blockchain is immutable and can't be modified. Tampering with any data is mathematically impossible.
Data destruction	Destroying any data or transactions that happened within the voting process may influence voting results and disrupt the audit process, concealing potential malicious actions.	All data in blockchain is immutable and can't be destroyed. Tampering with any data is mathematically impossible.

3.3 Compromising access to confidential data

Risk	Description	Mitigation
Unauthorized access to data independent of voting: positions, user identities.	Personal data is not intended to be revealed and may be of strategic significance to the shareholders. Revealing this data may allow perpetrators to exert influence in a way that is not intended by the law.	All private data is encrypted on the blockchain.
Unauthorized access to voting information (instructions,	Certain types of data are not intended to be revealed and may be used to deduce personal information or	All private data is encrypted on the blockchain. Behavioral patterns (e.g. votes from particular wallets towards particular outcomes) are

Risk	Description	Mitigation
proxies, vote counts) after the process.	decisions that were meant to remain hidden, which may allow perpetrators to exert influence in a way that is not intended by the law.	protected further using zero knowledge algorithms, which prevent unauthorized actors from deducing anything about them.
Unauthorized access to voting information (instructions, proxies, preliminary vote counts) during the process.	Gaining access to preliminary voting results will allow the perpetrator to vote tactically according to the situation, giving him an unfair advantage over other voters.	All private data is encrypted on the blockchain. Behavioral patterns (e.g. votes from particular wallets towards particular outcomes) are protected further using zero knowledge algorithms, which prevent unauthorized actors from deducing anything about them.

3.4 Infrastructure failure

Risk	Description	Mitigation
Loss of control over network	It may be possible for a perpetrator to take over the network or to disrupt its operation completely, preventing the network operator from fulfilling its responsibilities.	Each individual node of the network can be easily replicated anywhere as long as its private key is not compromised. Any compromised node only gives the perpetrator authority to perform actions valid for that node and the state of the system. Owner of each mode must take measures to protect its private keys from being compromised.
Denial of service	Voting process, like any other, is susceptible to denial of service attacks which can bring down key infrastructure nodes and prevent execution of business processes in a timely manner.	Each individual node of the network can be easily replicated anywhere without loss of data. The network can automatically rewrite its physical routing when that happens.
Difficulty of recovering trustworthy and	Regulators often change their requirements to processes in the financial industry, including	Blockchain supports having master keys with elevated read access rights, which can be given

Risk	Description	Mitigation
complete data for audit and regulation purposes.	shareholder voting. These changes create significant costs to alter the systems that can provide the data as required by regulators or auditors.	to the auditors or other parties which require this access. The blockchain stores all data that is significant for the process. If the regulatory requirements change, the regulators or auditors can adapt which data they retrieve from the chain to satisfy these requirements.

4. DATA ENTITIES IN DISTRIBUTED LEDGER

4.1 General considerations

This chapter describes on a high level all data entities that should be stored in an immutable distributed ledger. As described in the previous chapter, storing data in the ledger allows the system to provide certain guarantees to its users and to be the source of trust and thus reduces many of the traditional risks in the process. The copies of data stored in the ledger are the golden source of truth, and any replica of this data stored elsewhere is not considered valid if it is different from what is stored in the ledger.

Data stored in the distributed ledger can be classified into several distinct kinds:

- Regular data and metadata, stored on the network (e.g. meeting agenda information) or on the node (e.g. identification data). Access to this kind of data is defined in the same way as in traditional systems.
- Tokens. They are owned by the wallets in which they are stored and may be transferred by the owner of the wallet (and in some cases, other parties according to particular rules).
- Transactions, which are traces of token movement between wallets. They can never be created manually.

This classification emphasizes the differences on how the data can be perceived, accessed and acted upon.

4.2 Access Rights Considerations

Most data entities in the distributed ledger contain some kind of confidential information and must not be accessible without proper authorization. This chapter provides baseline considerations on which actors may access certain entities under certain conditions.

The Auditor role deserves a special mention. There are different kinds of auditors with different needs:

- Regulators, which may require full read access to all data, and possibly even the ability to execute certain administrative actions. Each regulator is certain to impose its own requirements to its access rights and they may be hard to predict on a global scale. For the sake of completeness, we assume that most regulators will want full read access on all entities and transactions.

- Auditors of the market participants, who perform audit on behalf of their employers. These auditors will need to have access rights corresponding to the access rights of their employer and may not have any higher access rights.
- Independent auditors, who perform the audit to prove the correctness of the process in general, without looking at any specific details. They don't need any access to confidential data and can work with the data that is available publicly.

Due to the nature of DLT, data can't be modified or deleted on the distributed ledger. Instead, if at any time it is necessary to modify or delete any piece of data, a separate new record is created, which also includes in itself a trait that invalidates the old record. The old record will remain visible and accessible on the network for all time. For the sake of brevity, every time we mention modification, deletion, amendment, update or similar operations, we assume that this mechanism is used.

4.3 Data Entity Descriptions

4.3.1 Meeting Agenda

The published agenda of the meeting. Includes data like:

- Key dates: meeting, record, market and agent deadlines
- Items for voting and discussion
- General information for participants

Agenda, along with the timing of the initial publication and any updates has legal significance in certain scenarios. It can be used as a source of truth of what information was available to all parties at what time.

Kind: regular data.

Issuer Agent	Intermediary	Voting Party
Create Amend Read	Read	Read

Note: availability of the amendment operation is subject to local regulations.

4.3.2 Meeting Parameters

The technical parameters of the meeting which are used by the chain code to enforce correctness of various calculations. Includes data like:

- How different share types are converted into voting rights
- Record date for position cut off
- Any other rules that may affect voting rights or outcomes

Meeting parameters are critical to both automation and to resolving any disputes. The system can be designed to calculate certain actions according to these parameters - it will be a calculation that will be both openly available and applied to everyone. Proving that certain parameters were used reduces or eliminates many risks in the voting process.

Kind: regular data.

Issuer Agent	**Intermediary**	**Voting Party**
Create Amend Read	Read	Read

Note: availability of the amendment operation is subject to local regulations.

4.3.3 Agenda Proposal Artifacts

All artifacts from the process of proposing and approving new agenda items:

- Proposals
- Approvals/rejections
- Any other relevant traces of the process

If the agenda proposal extension is implemented, the entire proposal processes must be recorded on the blockchain to settle disputes in the future. The functionality is described in requirements №20-30. Exact artifacts and access rights depend on implementation.

Kind: depending on implementation, may be regular data or tokens + transactions.

Issuer Agent	Intermediary	Voting Party
Create	Read	Create
Amend		Amend
Read		Read only own confidential data

4.3.4 Holding Records

Records of shares held by shareholders on a certain date (typically record date). Includes data like:

- Attachment to a Voting Party
- Date and units held

Holding records are the initial source of data that drives the voting process. Any discrepancies in data are reconciled on this level, before applying any further calculations to them. It minimizes the risks and simplifies the reconciliation process. Since reconciliation differences at this level are very common, it is important that all loaded positions and reconciliation adjustments are stored on the chain to minimize dispute and reduce risks.

Kind: regular data, attached to a node.

Issuer Agent	Intermediary	Voting Party
Create	Create	Read only own confidential data
Amend	(optional) Amend	
Read	Read only confidential data for Voting Parties served by itself or by lower tier Intermediaries	

Note: creation rights may be limited for Issuer Agent and/or Intermediary depending on how reconciliation process is implemented. Amendment is subject to implementation choices and local regulations and may be very limited or not allowed at all.

4.3.5 Voting Party Identification

Proof that the Voting Party is identified and his personal data can be retrieved at a secured location by an authorized party. May include a hash of personal data, a link to an internal storage at the authentication center or a similar piece of data.

The voting process requires user identification to work, but the identities typically can't be stored on the blockchain due to data privacy laws in many countries. They will typically be stored off-chain in a secure storage at the authentication center, and the data stored in the blockchain (like a hash) must provide a way to retrieve this data for the authorized parties.

Kind: regular data, attached to a node.

Issuer Agent	Intermediary	Voting Party
Read	Create Read only confidential data for served Voting Parties	Read only own confidential data

4.3.6 Voting Rights

Tokens that are used to perform many actions related to voting, including giving out proxy rights and the voting itself. They don't include much data other than a trace of why they were issued.

Voting Right is a token that is critical to the process. While it doesn’t store much data itself, its ownership by a node and transactions that transfer it from one node to another describe a large part of the voting process. These transactions must be possible to follow up in case of disputes to reduce or eliminate many risks.

Kind: token.

Issuer Agent	Intermediary	Voting Party
Create Read Verify integrity (zero knowledge proof)	Verify integrity (zero knowledge proof)	Read only own confidential data Verify integrity (zero knowledge proof)

4.3.7 Proxy Assignments

Transactions that record transfer of voting rights from one party to another. Include source, destinations and possibly any custom proxy-related process data.

Proxy assignment is a key piece of the process and must remain traceable in any case of disputes.

Kind: transactions (movements of Voting Rights).

Issuer Agent	Intermediary	Voting Party
Read public data Verify integrity (zero knowledge proof)	Read public data	Create Read only own confidential data Verify integrity (zero knowledge proof)

4.3.8 Voting Instructions

Transactions that record the choice made during the voting. Include the Voting Party and the desired vote outcome.

Issuing instructions is the main piece of the voting process. It must remain traceable in any case of disputes.

Kind: transactions (movements of Voting Rights).

Issuer Agent	Intermediary	Voting Party
Read Verify integrity (zero knowledge proof)	Verify integrity (zero knowledge proof)	Create Read only own confidential data Verify integrity (zero knowledge proof)

4.3.9 Meeting Minutes

Documented events that happened at the meeting. The data may include:

- Discussions held at the meeting
- Statements by the company management
- Links to supplementary materials like video recording of the meeting

Alongside the e-voting process, the general meeting is still run in some physical place, likely supplemented by online involvement (e.g. voting online during the meeting). Apart

from the voting itself, there are many things of note that happen during the meeting which may be of significance in case of disputes, and should be preserved in the blockchain.

Kind: regular data.

Issuer Agent	Intermediary	Voting Party
Create Amend (within functional restrictions) Read	Read	Read

Note: extension functionality. Availability of the amendment operation is subject to local regulations.

4.3.10 Administrative Adjustments

Transactions taken by the meeting administrator (or another authorized party) that alter the results of the voting process. Must include the content of the adjustment, reasoning behind it and link to any parties whose votes were adjusted.

In case the administrator is legally allowed to adjust or arrest votes, these adjustment actions must be very clearly traceable and visible to both auditors and the involved Voting Parties. Disputes that will likely follow the adjustments must be based on the clear data of what adjustment was issued and why.

Kind: regular data.

Issuer Agent	Intermediary	Voting Party
Create Read	Read	Read

4.3.11 Meeting Results

Summarized and published outcome of the meeting, including all voting results.

Meeting results are automatically generated as a summary of the outcomes of all items on the agenda. They are perceived as the legally binding outcome of the meeting and carry the most significance after the meeting out of all artifacts stored on the ledger.

Kind: regular data.

Issuer Agent	Intermediary	Voting Party
Read	Read	Read

Note: Meeting results are generated automatically by the system and cannot be changed in any way by any actor.

5. NON-FUNCTIONAL REQUIREMENTS

5.1 Availability

The system must be available 24/7/365.

5.2 Data Integrity

The system must provide audit trails. The audit trails must be easily retrievable and understandable for all appropriate parties according to the local legislation.

5.3 IT Environment

The system must be deployable in the following environments:

- Development – internal testing
- QA – market testing
- Production – primary and secondary sites running in active-active configuration

5.4 Interoperability

The system must interact with other systems (including those that are a part of the standard solution) via documented open APIs.

5.5 Performance

The response time for the whole solution must be under a second from click to on-screen response.

5.6 Recoverability

In the worst case scenario it must be possible to recover the system to a valid state no later than within one day.

5.7 Regulatory

System must not introduce any new process risks over the currently available systems.

5.8 Reliability

The system must have an active-active failover cluster, without dependency on any single node.

5.9 Scalability

- The system must be able to scale to accommodate meeting sizes of up to 100,000 voting parties.
- The system must be able to handle at least 50 transactions per second.
- The system must handle multiple independent meetings running in parallel.

5.10 Security

- Cryptographic key management must support HSMs.
- The system must be compliant with the relevant best practices in information security.

5.11 Usability

- The system must provide a responsive web interface that can be used on smartphones, tablets, and regular PCs.
- The system must provide a user-friendly learning mechanism for the new users, e.g. in-app tutorials.

6. FUTURE DEVELOPMENTS

This document is a work in progress that is maintained by the CSD Working Group on DLT. Future versions will include but are not limited to:

- wider coverage of the international market, including more countries,
- deeper alignment with existing international standards, e.g. ISO20022,
- complete requirements for a cross-system and cross-border integration solution,
- … and more.

The work outlined in this document is innovative in its nature. The members of the working group hope that this document will be useful to the wide range of market participants in understanding, implementing and standardizing DLT solutions of all kinds and in the field of e-proxy voting in particular.

7. DISTRIBUTION AND CONTACTS

This document may be shared by the member organizations of the working group freely with the interested parties. The working group welcomes feedback on the contents of the document as well as proposals for cooperation on any further work.

To get in touch with the working group, please contact:

- Alexander Chekanov, NSD, chekanov.as@nsd.ru
- Tanya Knowles, Strate, tanyak@strate.co.za
- Urs Sauer, SIX Securities Services, urs.sauer@six-group.com
- Michael Rexestrand, Nasdaq, michael.rexestrand@nasdaq.com
- Claudio Calderón, DCV, claudio.calderon@dcv.cl

The alignment of this work with the ISO20022 has been prepared in deep collaboration with SWIFT. To get in touch with them, please contact:

- Cécile Dessambre, SWIFT, cecile.dessambre@swift.com