Pi-Vote Protocol Documentation

Pi-Vote Doc Generator, Pirate Party Switzerland
Stefan Thöni, Pirate Party Switzerland

Steinhausen, September 29, 2011, Version 1.1.4.0

Contents

1 RPC Protocol

Pi-Vote uses an Remote Procedure Call protocol over TCP. To establish communication the client opens a TCP connection to the server. All action is initiated by the client sending a request. The server processes these request and answers each one with a response.

1.1 Messages

Both request and response are messages which use a common transmission format.

Part	**Type**	**Usage**
Length	Int32	Contains the length of the following data.
Data	Byte[]	Contains the serialized message data.

1.2 Example

Exampele of a keep alive request.

Hex bytes	Comment
” 37 00 00 00	Length of the following data.
22 50 69 72 61 74 65 2e 50 69 56 6f 74 65 2e 52 70 63 2e 4b 65 65 70 41 6c 69 76 65 52 65 71 75 65 73 74	String ’Pirate.PiVote.Rpc.KeepAliveRequest’ in UTF8 with prefixed length.
10 00 00 00 09 35 5d d3 9a b9 8a 41 96 e0 41 18 82 a5 85 90	Request Guid as 16 bytes with prefixed length.

And the corresponding keep alive response:

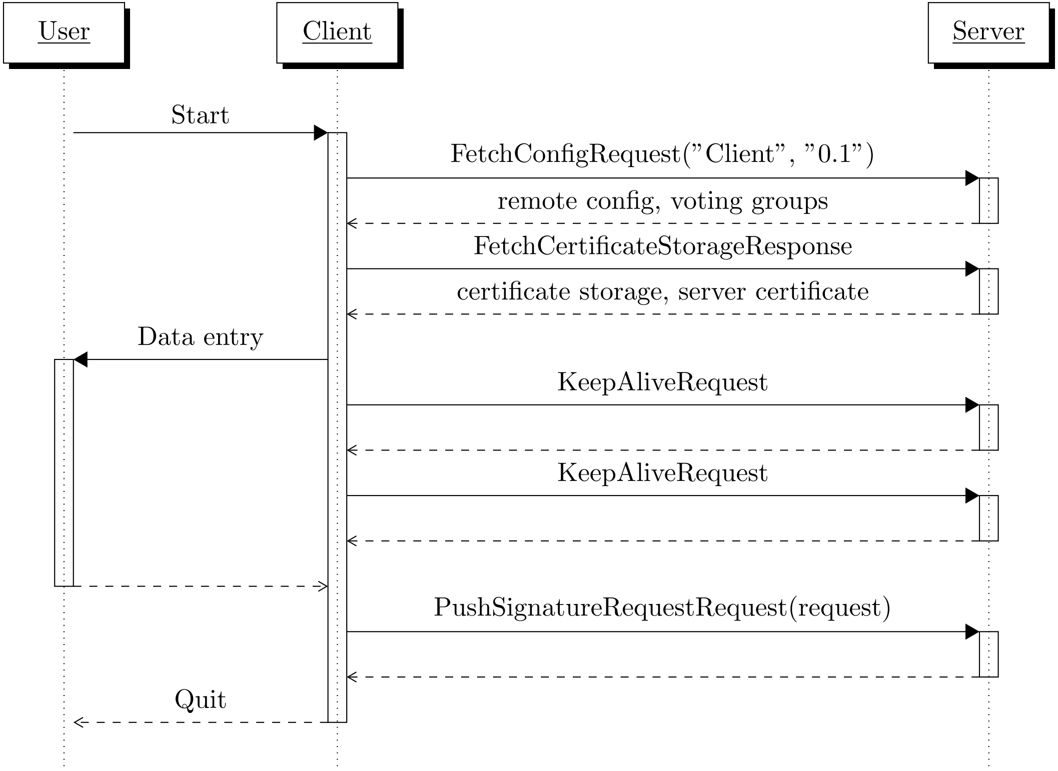
Hex bytes	Comment
39 00 00 00	Length of the following data.
23 50 69 72 61 74 65 2e 50 69 56 6f 74 65 2e 52 70 63 2e 4b 65 65 70 41 6c 69 76 65 52 65 73 70 6f 6e 73 65	String ’Pirate.PiVote.Rpc.KeepAliveResponse’ in UTF8 with prefixed length.
10 00 00 00 09 35 5d d3 9a b9 8a 41 96 e0 41 18 82 a5 85 90	Request Guid as 16 bytes with prefixed length.
01	Boolean specifying that no exception occurred in execution.

2 Sequences

This section shows common sequences in the Pi-Vote process. Beware that these diagrams do not show where to encrypt, decrypt, sign or verify what with what certificate. Please consult the request list in the next section for this information.

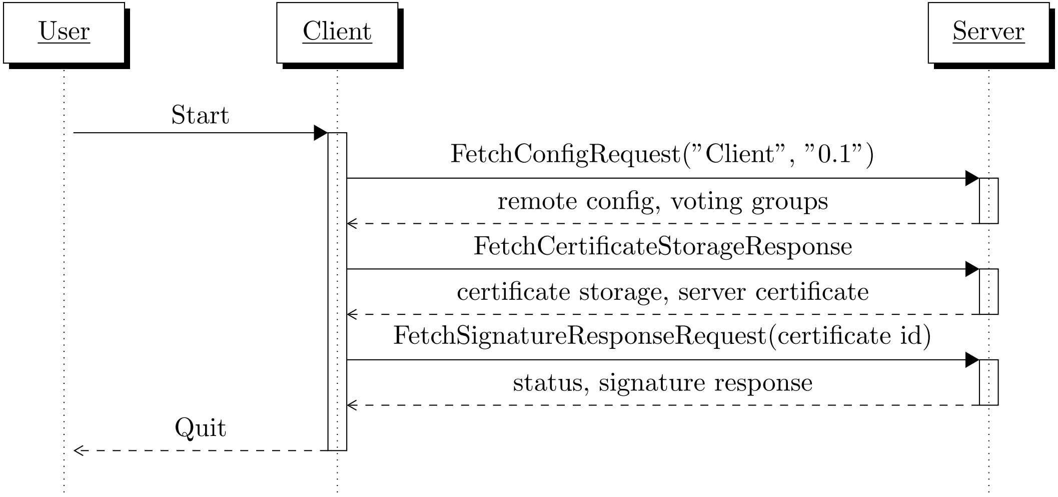
2.1 Request certificate signing

How the client can get all nessecary data, create his certificate signing request and upload this to the server.


User
Client
Server
Start
FetchConfigRequest(”Client”, ”0.1”)
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
Data entry
KeepAliveRequest
KeepAliveRequest
PushSignatureRequestRequest(request)
Quit

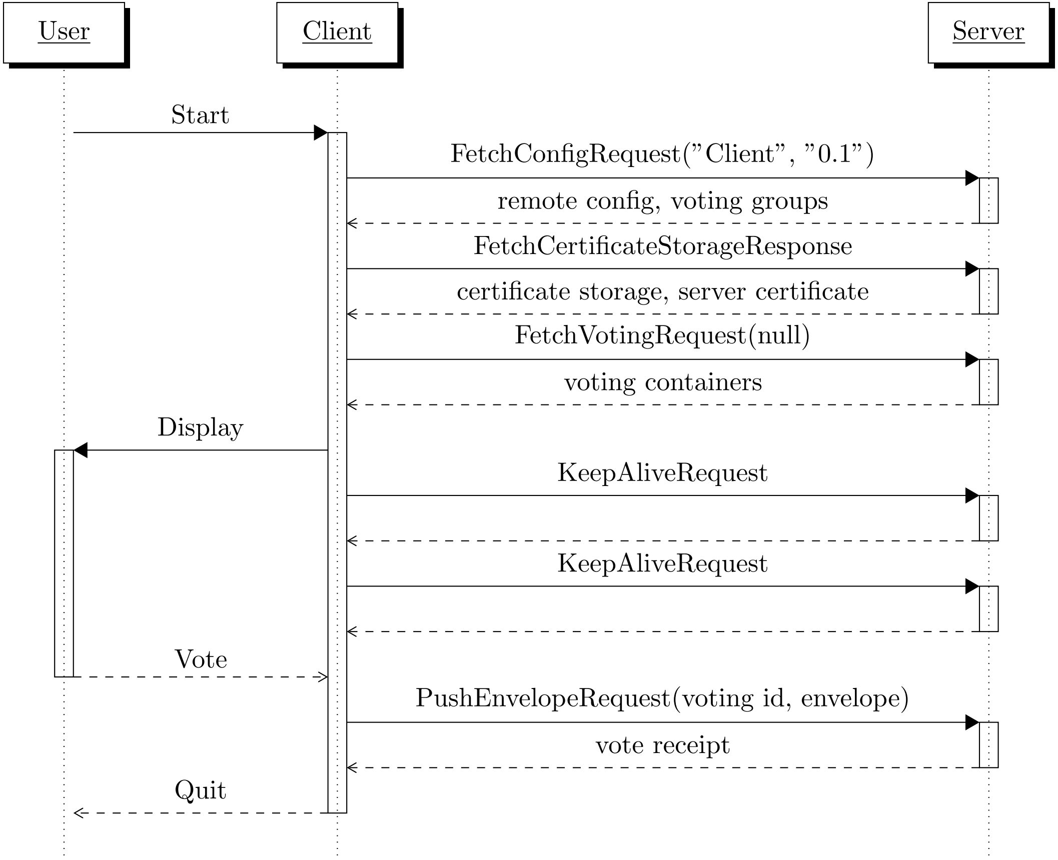
2.2 Get response to signing request

How the client can detect when the signature response is available and fetch it.


User
Client
Server
Start
FetchConfigRequest(”Client”, ”0.1”)
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
FetchSignatureResponseRequest(certificate id)
status, signature response
Quit

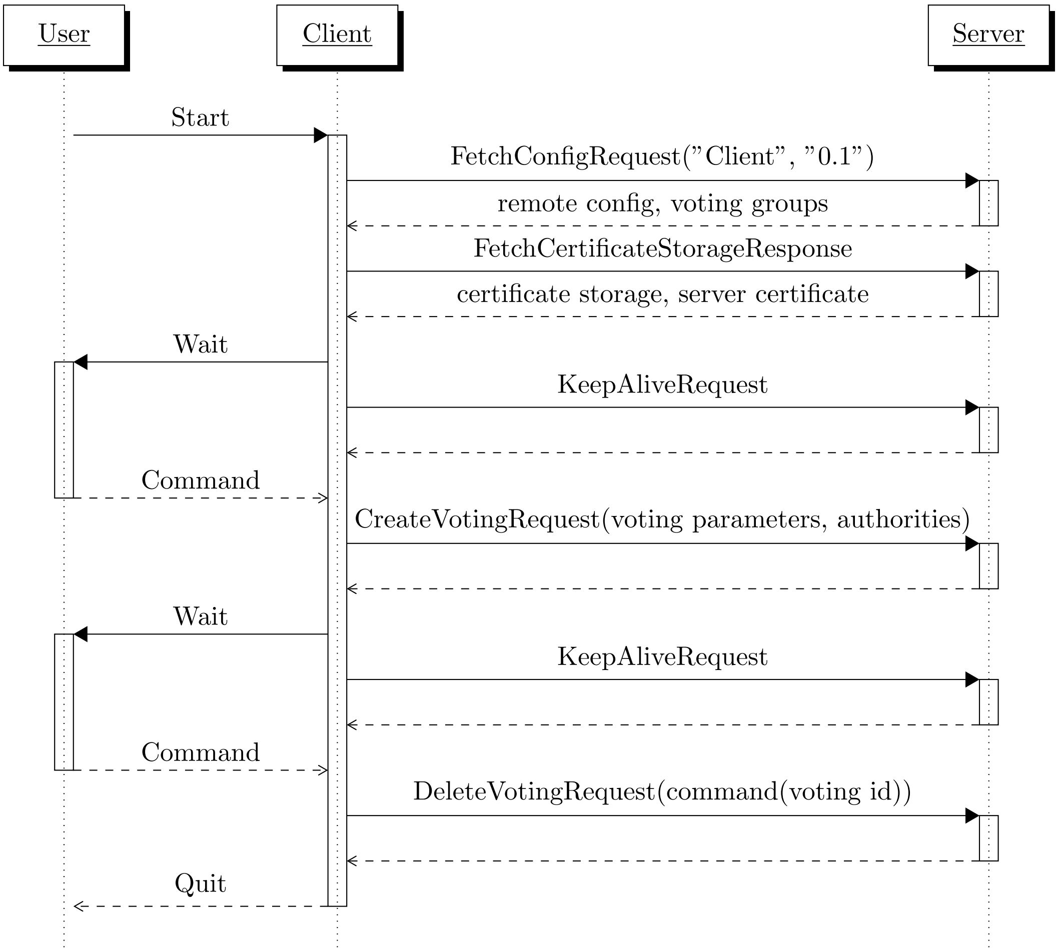
2.3 Cast a vote

How the client can get all nessecary data and then cast a vote.


User
Client
Server
Start
FetchConfigRequest("Client", "0.1")
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
FetchVotingRequest(null)
voting containers
Display
KeepAliveRequest
KeepAliveRequest
Vote
PushEnvelopeRequest(voting id, envelope)
vote receipt
Quit

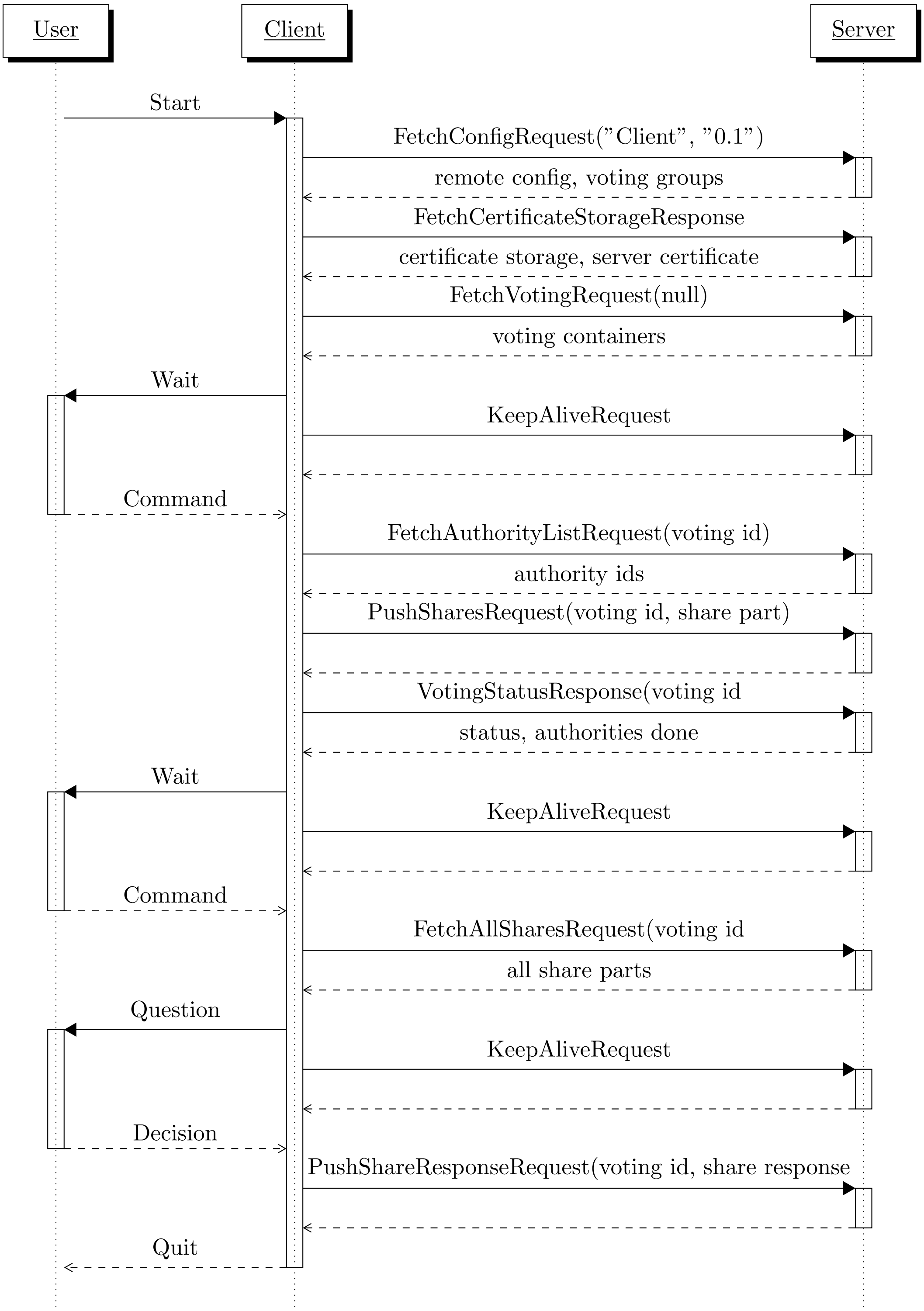
2.4 Create and delete a voting

How the client can create a voting and then delete it again.


User
Client
Server
Start
FetchConfigRequest(”Client”, ”0.1”)
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
Wait
KeepAliveRequest
Command
CreateVotingRequest(voting parameters, authorities)
Wait
KeepAliveRequest
Command
DeleteVotingRequest(command(voting id))
Quit

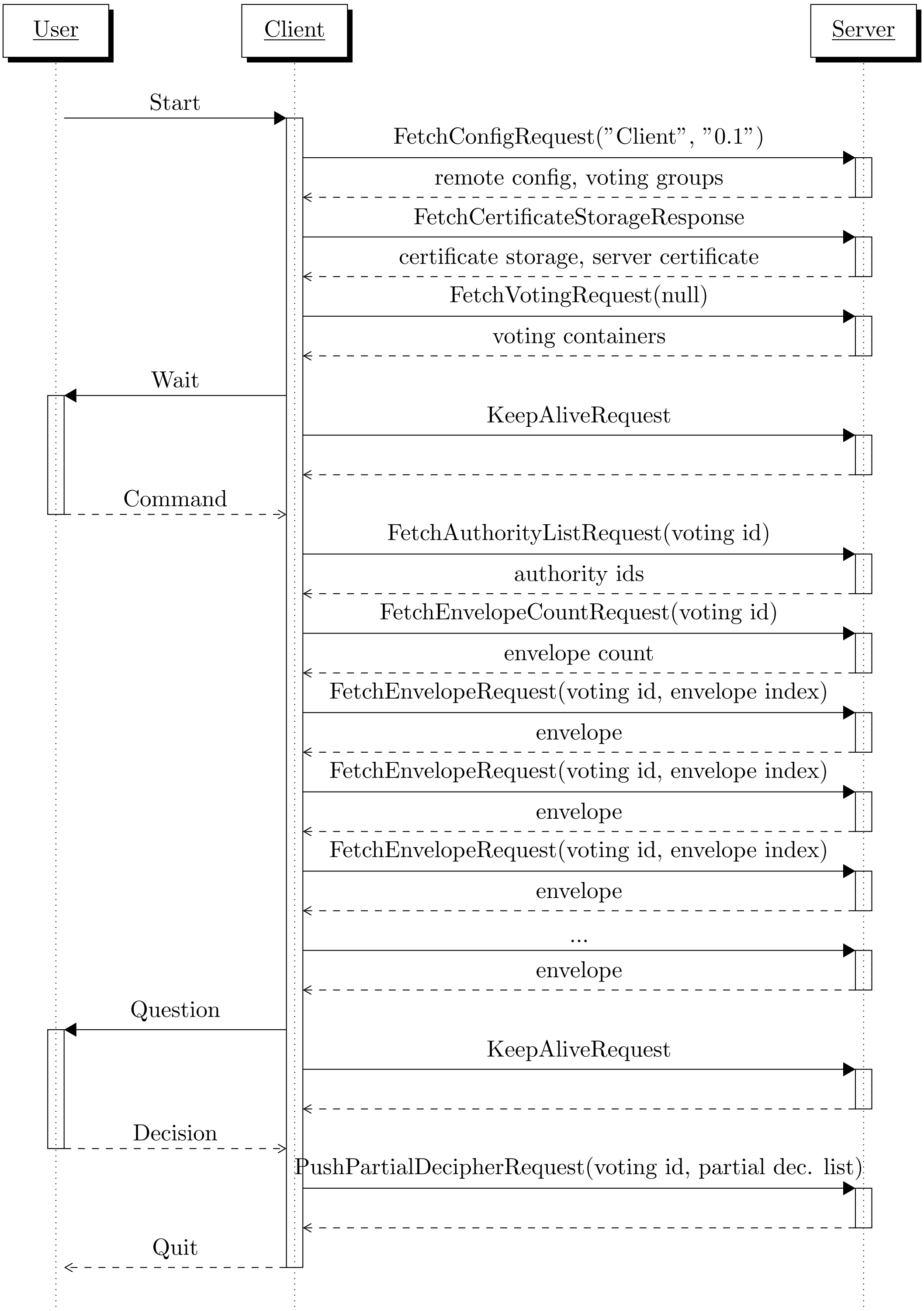
2.5 Depsit share part and share response

How the client can deposit an authorities share part and share response. This assumes that the authority is the last one to deposit the share part so it can move on to the response immediatly.


User
Client
Server
Start
FetchConfigRequest(”Client”, ”0.1”)
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
FetchVotingRequest(null)
voting containers
Wait
KeepAliveRequest
Command
FetchAuthorityListRequest(voting id)
authority ids
PushSharesRequest(voting id, share part)
VotingStatusResponse(voting id
status, authorities done
Wait
KeepAliveRequest
Command
FetchAllSharesRequest(voting id
all share parts
Question
KeepAliveRequest
Decision
PushShareResponseRequest(voting id, share response
Quit

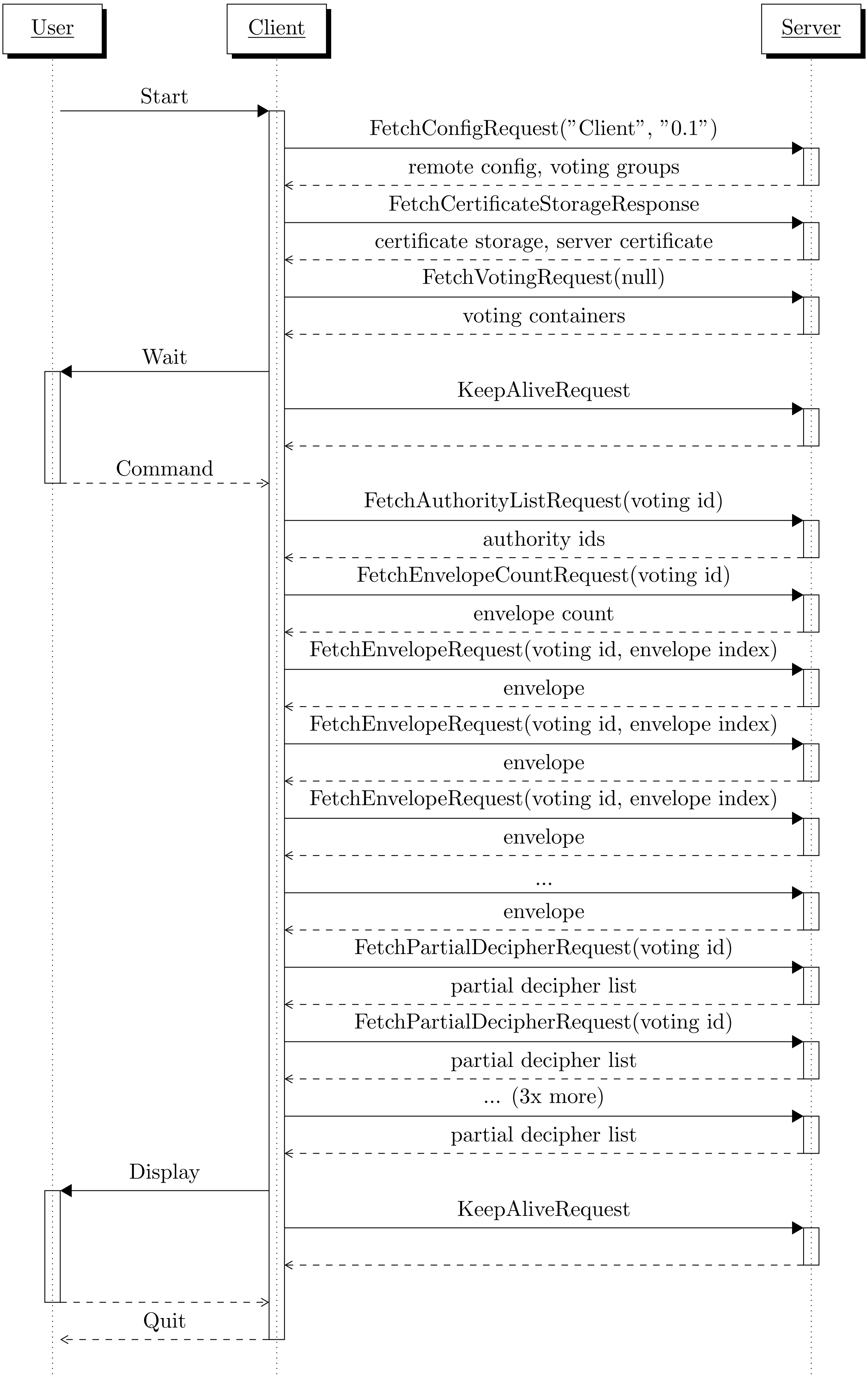
2.6 Tally voting an publish decipher part

How the client can tally a voting and upload the decipher parts. It needs to download all envelopes and sum them up, partially decrypt the sum and upload the partial deciphers.


User
Client
Server
Start
FetchConfigRequest(”Client”, ”0.1”)
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
FetchVotingRequest(null)
voting containers
Wait
KeepAliveRequest
Command
FetchAuthorityListRequest(voting id)
authority ids
FetchEnvelopeCountRequest(voting id)
envelope count
FetchEnvelopeRequest(voting id, envelope index)
envelope
FetchEnvelopeRequest(voting id, envelope index)
envelope
FetchEnvelopeRequest(voting id, envelope index)
envelope
...
envelope
Question
KeepAliveRequest
Decision
PushPartialDecipherRequest(voting id, partial dec. list)
Quit

2.7 Tally voting an display the result

How the client can tally a voting and calculate the result. It needs to download all envelopes and sum them up, then download all decipher parts and decipher the result.


User
Client
Server
Start
FetchConfigRequest(”Client”, ”0.1”)
remote config, voting groups
FetchCertificateStorageResponse
certificate storage, server certificate
FetchVotingRequest(null)
voting containers
Wait
KeepAliveRequest
Command
FetchAuthorityListRequest(voting id)
authority ids
FetchEnvelopeCountRequest(voting id)
envelope count
FetchEnvelopeRequest(voting id, envelope index)
envelope
FetchEnvelopeRequest(voting id, envelope index)
envelope
FetchEnvelopeRequest(voting id, envelope index)
envelope
...
envelope
FetchPartialDecipherRequest(voting id)
partial decipher list
FetchPartialDecipherRequest(voting id)
partial decipher list
... (3x more)
partial decipher list
Display
KeepAliveRequest
Quit

3 Requests

The following request are used to upload and download data from the Pi-Vote server. For detailed data types, consult the Types section.

Type	CreateVotingRequest
Text	Tells the server to create a new voting procedure.
Input	Voting parameters signed by an admin certificate, list of 5 authorities

Type	DeleteVotingRequest
Text	Tells the server to delete a voting.
Input	Embedded command object with id of the voting signed by an admin certificate.

Type	EndVotingRequest
Text	Tells the server to and a voting. This request is no longer supported.

Type	FetchAllSharesRequest
Text	Downloads all authority key shares for a voting from the server.
Input	Id of the voting.
Output	All share parts in a single container.

Type	FetchAuthorityCertificatesRequest
Text	Downloads all valid authority certificate from the server. This is done in preperation for creating a voting.
Output	List of all valid authority certificates.

Type	FetchAuthorityListRequest
Text	Donloads the certificate from all authorites in a certain voting from the server.
Input	Id of the voting.
Output	List of all authorities in that voting.

Type	FetchCertificateStorageRequest
Text	Fetches the certificate storage and the server certificate from the server. This is done upon start of the client to get the nessecary date to validate certificates.
Output	Certificate storage with all CAs and CRLs, server certificate.

Type	FetchConfigRequest
Text	Downloads the config and the voting groups from the server. Also tells the server what kind of client is connected. This is the first message as it also contains information about updates.
Input	Name of the client program, version of the client program.
Output	Remote configuration for the client, list of voting groups.

Type	FetchEnvelopeCountRequest
Text	Gets the number of envelopes in a voting. This is done before downloading the votings.
Input	Id of the voting.
Output	Number of envelopes in that voting.

Type	FetchEnvelopeRequest
Text	Downloads an envelope from the server by stating the voting and index of the envelope.
Input	Id of the voting, index of an envelope.
Output	Envelope signed by the voter.

Type	FetchParametersRequest
Text	Gets the parameters for a voting together with the index of an authority in a voting. This is used by the authorities.
Input	Id of the voting, certificate of an authority.
Output	Index of stated authority, voting material.

Type	FetchPartialDecipherRequest
Text	Downloads list of partial decipehrs from an authority for a specified voting. This is done when tallying a voting.
Input	Id of the voting, index of an authority.
Output	Partial decipher list signed by that authority.

Type	FetchSignatureRequestListRequest
Text	Downloads a list of ids of the pending signature requests. This is done by an administrator when downloading signature requests.
Output	List of guid of the pending signature requests.

Type	FetchSignatureRequestRequest
Text	Downloads a list of ids of the pending signature requests. This is done by an administrator when downloading signature requests.
Input	Id of a signature request.
Output	Signature request encrypted for the CA and signed by the requester.

Type	FetchSignatureResponseRequest
Text	Downloads the CA's response to a signature request.
Input	Id of the signature request.
Output	Status of the signature request, signature response signed by the CA.

Type	FetchSignCheckCookieRequest
Text	Download a sign check cookie.
Input	Id of the notary or authority certificate, code to access the sign check cookie.
Output	Sign check cookie signed by the notary or authority.

Type	FetchSignCheckListRequest
Text	Download the list of sign checks for a certificate.
Input	Id of the certificate.
Output	List of signature request sign checks signed by the web server.

Type	FetchVotingMaterialVoterRequest
Text	Downloads voting materials and status for several votings at once.
Input	List of ids of votings or null list for all votings.
Output	List of tuples containing voting material, voting status and a list of ids of the involved authorites.

Type	FetchVotingRequest
Text	Downloads all important data for serveral votings at once.
Input	List of ids of votings or null list for all votings.
Output	List of voting containers.

Type	KeepAliveRequest
Text	Does nothing but keep the connection alive.

Type	ListVotingIdsRequest
Text	Fetches the ids of all votings.
Output	List of ids of votings.

Type	PushCertificateStorageRequest
Text	Uploads a certificate storage which will be merge into the server database.
Input	A certificate storage including CAs and CRLs.

Type	PushEnvelopeRequest
Text	Cast a vote by uploading an envelope.
Input	Id of the voting, envelope signed by the voter.
Output	Receipt for the voter signed by the server.

Type	PushPartialDecipherRequest
Text	Uploads partials deciphers from an authority.
Input	Id of the voting, partial decipher list signed by the authority.

Type	PushShareResponseRequest
Text	Uploads an authority's response to the sharing.
Input	Id of the voting, share response signed by the authority.

Type	PushSharesRequest
Text	Uploads the share part from an authority.
Input	Id of the voting, share part signed by the authority.

Type	PushSignatureRequestRequest
Text	Uploads a request for a signature on a certificate by the CA.
Input	Signature request encrypted for the CA and signed by the requester, auxiliary signature information encrypted for the server and signed by the requester.

Type	PushSignatureResponseRequest
Text	Uploads a signature response from the CA.
Input	Signature response signed by the CA.

Type	PushSignCheckCookieRequest
Text	Uploads a sign check cookie from a notary or authority.
Input	Sign check cookie signed by the notary or authority.
Output	Code encrypted for the notary or authority.

Type	PushSignCheckRequest
Text	Uploads a sign check from a notary or authority.
Input	Signature request sign check signed by the web server.

Type	VotingStatusRequest
Text	Gets the status of a voting.
Input	Id of the voting.
Output	Status of the voting, list of the authorities which have completed the current phase.

4 Types

The following type formats are used for messages and other containers contained in messages.

4.1 Basic Types

The following basic types are used throughout Pi-Vote.

Type	Emil.GMP.BigInt
Serialize	Arbitrary-sized integer as specified by GNU Multiprecision Library written as Byte[]

Type	Pirate.PiVote.MultiLanguageString
Short	MultiLanguageString
Serialize	Number of language entries as Int32 followed by each entry as Language as Int32 and String text

Type	Pirate.PiVote.PiException
Short	PiException
Serialize	Exception code as Int32 followed by String message.

Type	System.Boolean
Short	Boolean
Serialize	1 byte boolean written as 0 when false and 1 when true

Type	System.Byte
Short	Byte
Serialize	Just one byte

Type	System.Byte[]
Short	Byte[]
Serialize	UInt32 length followed by the individual bytes.

Type	System.DateTime
Short	DateTime
Serialize	Number of 100-nanosecond intervals that have elapsed since 12:00:00 midnight, January 1, 0001 written as Int64

Type	System.Double
Short	Double
Serialize	8 byte floating point written as per IEEE 754

Type	System.Guid
Short	Guid
Serialize	16 byte Globally Unique Identifier written as Byte[]

Type	System.Int32
Short	Int32
Serialize	4 byte signed integer written in little endian format

Type	System.Int64
Short	Int64
Serialize	8 byte signed integer written in little endian format

Type	System.Single
Short	Single
Serialize	4 byte floating point written as per IEEE 754

Type	System.String
Short	String
Serialize	UInt32 length followed by UTF8 encoded string data

Type	System.UInt32
Short	UInt32
Serialize	4 byte unsigned integer written in little endian format

Type	System.UInt64
Short	UInt64
Serialize	8 byte unsigned integer written in little endian format

4.2 List Types

The following list types are used. They are all generic an can contains any number of items.

Type	System.Collections.Generic.Dictionary
Short	Collections.Generic.Dictionary
Serialize	Number of entries followed by the serialization of each key and value

Type	System.Collections.Generic.List
Short	Collections.Generic.List
Serialize	Number of entries followed by the serialization of each entry

4.3 Enumerations

The following enumerations are used. The values and their names are specified below.

Type	Pirate.PiVote.Crypto.CertificateAttributeName	
Short	Crypto.CertificateAttributeName	
Comment	Name of the certificate attribute.	
Values	None	0
	GroupId	1
	Language	2

Type	Pirate.PiVote.Crypto.PrivateKeyStatus	
Short	Crypto.PrivateKeyStatus	
Comment	Status of a private key.	
Values	Unavailable	0
	Unencrypted	1
	Encrypted	2
	Decrypted	3

Type	Pirate.PiVote.Crypto.SignatureResponseStatus	
Short	Crypto.SignatureResponseStatus	
Comment	Status of the signature response.	
Values	Unknown	0
	Pending	1
	Accepted	2
	Declined	3

Type	Pirate.PiVote.Crypto.VotingStatus	
Short	Crypto.VotingStatus	
Comment	Status of the voting procedure.	
Values	New	0
	Sharing	1
	Voting	2
	Aborted	3
	Ready	4
	Deciphering	5
	Finished	6
	Offline	7

Type	Pirate.PiVote.ExceptionCode	
Short	ExceptionCode	
Comment	Codes for identifiing exceptions.	
Values	Unknown	0
	ArgumentNull	1
	ArgumentOutOfRange	2
	BadSerializableFormat	3
	InvalidCertificate	4
	WrongStatusForOperation	5
	RequestSignatureInvalid	6
	NoAuthorizedAdmin	7
	BadVotingMaterial	8
	InvalidSignature	9
	InvalidSignatureRequest	10
	ServerCertificateInvalid	11
	CanceledByUser	12

	AuthorityCountOutOfRange	1000001
	TheresholdOutOfRange	1000002
	OptionCountOutOfRange	1000003
	MaxVotaOutOfRange	1000004
	OptionCountMismatch	1000005
	PIsNoPrime	1000006
	PIsNoSafePrime	1000007
	QIsNoPrime	1000008
	AuthorityCountMismatch	1000009
	AuthorityInvalid	1000010
	NoVotingWithId	2000001
	NoAuthorityWithCertificate	3000001
	AlreadyVoted	4000001
	VoteSignatureNotValid	4000002
	NoVoterCertificate	4000003
	InvalidVoteReceipt	4000004
	BadGroupIdInCertificate	4000005
	InvalidEnvelope	4000006
	InvalidEnvelopeBadDateTime	4000007
	InvalidEnvelopeBadVoterId	4000008
	InvalidEnvelopeBadBallotCount	4000009
	InvalidEnvelopeBadProofCount	4000010
	InvalidEnvelopeBadVoteCount	4000011
	SignatureRequestInvalid	5000001
	SignatureRequestResponded	5000002
	SignatureRequestNotFound	5000003
	SignatureResponseNotFromCA	6000001
	NoAuthorizedAuthority	7000001
	AlreadyEnoughAuthorities	7000002
	AuthorityAlreadyInVoting	7000003
	AuthorityHasAlreadyDeposited	7000004
	PartialDecipherBadSignature	8000001
	PartialDecipherBadEnvelopeCount	8000002
	PartialDecipherBadEnvelopeHash	8000003
	ShareResponseBadSignature	9000001
	ShareResponseWrongAuthority	9000002
	ShareResponseNotAccepted	9000003
	ShareResponseParametersDontMatch	9000004
	CommandNotFromAdmin	19000001
	CommandNotAllowedInStatus	19000002
	SignCheckCookieCodeWrong	20000001
	SignCheckCookieCodeExpired	20000002
	SignCheckCookieNotFound	20000003
	SignCheckCookieNotFromNotary	20000004
	SignCheckCookieSignatureInvalid	20000005
	SignCheckCookieFingerprintMismatch	20000006
	SignCheckCookieRandomnessMismatch	20000007
	SignCheckNotFromServer	21000001
	SignCheckResponseStateMismatch	21000002

Type	Pirate.PiVote.Language	
Short	Language	
Comment	Language of the interface and texts.	
Values	English	0

	German	1
	French	2
	Italien	3

Type	Pirate.PiVote.Rpc.VoteReceiptStatus	
Short	Rpc.VoteReceiptStatus	
Comment	Status of a vote receipt to check.	
Values	NotFound	0
	FoundBad	1
	FoundOk	2

4.4 Objects

The following composite types are used. They inherit their fields from one another.

Type Name	Pirate.PiVote.Crypto.AdminCertificate
Short Name	Crypto.AdminCertificate
Inherits	Crypto.Certificate
Comment	Certificate of a voting administrator.
Field Type	String
Field Name	FullName
Comment	Full name of the administrator.

Type Name	Pirate.PiVote.Crypto.AllShareParts
Short Name	Crypto.AllShareParts
Inherits	Serialization.Serializable
Comment	Assembly of all share parts from all authorities.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting procedure.
Field Type	Collections.Generic.List[Crypto.Signed[Crypto.SharePart]]
Field Name	ShareParts
Comment	Share parts from all authorities.

Type Name	Pirate.PiVote.Crypto.AuthorityCertificate
Short Name	Crypto.AuthorityCertificate
Inherits	Crypto.Certificate
Comment	Certificate of a voting authority.
Field Type	String
Field Name	FullName
Comment	Full name of the authority.

Type Name	Pirate.PiVote.Crypto.AuthorityList
Short Name	Crypto.AuthorityList
Inherits	Serialization.Serializable
Comment	List of all authorities in the voting procedure.
Field Type	Int32
Field Name	VotingId
Comment	Id of the voting procedure.
Field Type	Collections.Generic.List[Crypto.Certificate]
Field Name	Authorities
Comment	List of all authorities in the voting procedure.
Field Type	Collections.Generic.List[Crypto.Certificate]
Field Name	Certificates
Comment	Intermediate certificates.
Field Type	Collections.Generic.List[Crypto.Signed[Crypto.RevocationList]]
Field Name	RevocationLists
Comment	Certificate revocation list for CAs.

Type Name	Pirate.PiVote.Crypto.BadShareProof
Short Name	Crypto.BadShareProof
Inherits	Serialization.Serializable
Comment	Proof of a bad sharing.
Field Type	Int32
Field Name	ComplainingAuthorityIndex
Comment	Index of the complaining authority.

Field Type	Crypto.CertificateStorage
Field Name	CertificateStorage
Comment	Certificate storage.
Field Type	Crypto.Signed[Crypto.VotingParameters]
Field Name	SignedParameters
Comment	Signed voting parameters.
Field Type	Crypto.AllShareParts
Field Name	AllShareParts
Comment	All share parts.
Field Type	Collections.Generic.Dictionary[Int32, Crypto.TrapDoor]
Field Name	TrapDoors
Comment	Trap doors.
Field Type	Collections.Generic.Dictionary[Int32, Crypto.Certificate]
Field Name	Authorities
Comment	Involved authorities.

Type Name	Pirate.PiVote.Crypto.Ballot
Short Name	Crypto.Ballot
Inherits	Serialization.Serializable
Comment	Container for all votes from a voter.
Field Type	Collections.Generic.List[Crypto.Vote]
Field Name	Votes
Comment	Votes for each option.
Field Type	Collections.Generic.List[Crypto.Proof]
Field Name	SumProves
Comment	Proofs of sum of votes cast.

Type Name	Pirate.PiVote.Crypto.BaseParameters
Short Name	Crypto.BaseParameters
Inherits	Serialization.Serializable
Comment	Base for the voting parameters.
Field Type	Emil.GMP.BigInt
Field Name	P
Comment	Safe Prime.
Field Type	Emil.GMP.BigInt
Field Name	Q
Comment	Prime.
Field Type	Emil.GMP.BigInt
Field Name	G
Comment	Order Q element of Zp*.
Field Type	Emil.GMP.BigInt
Field Name	F
Comment	Element of ¡G¿.
Field Type	Int32
Field Name	Thereshold
Comment	Number of adversaries that can be tolerated.
Field Type	Int32
Field Name	AuthorityCount
Comment	Number of authorities.
Field Type	Int32
Field Name	ProofCount
Comment	Number of proves required to proof a single fact.

Field Type	Collections.Generic.List[Crypto.Question]
Field Name	Questions
Comment	Questions in the voting.

Type Name	Pirate.PiVote.Crypto.BooleanCertificateAttribute
Short Name	Crypto.BooleanCertificateAttribute
Inherits	Crypto.CertificateAttribute[TValue]
Comment	Boolean attribute of certificate.

Type Name	Pirate.PiVote.Crypto.CACertificate
Short Name	Crypto.CACertificate
Inherits	Crypto.Certificate
Comment	Certificate of a certificate authority.
Field Type	String
Field Name	FullName
Comment	Full name of the certificate authority.

Type Name	Pirate.PiVote.Crypto.Certificate
Short Name	Crypto.Certificate
Inherits	Serialization.Serializable
Comment	Certificate of identity.
Field Type	Byte[]
Field Name	MagicTypeConstant
Comment	The magic certificate type.
Field Type	Guid
Field Name	Id
Comment	Id of the certificate.
Field Type	DateTime
Field Name	CreationDate
Comment	Date of creation of this certificate.
Field Type	Byte[]
Field Name	PublicKey
Comment	Public key of the certificate.
Field Type	Byte[]
Field Name	SelfSignature
Comment	Signature from the certificate itself.
Field Type	Collections.Generic.List[Crypto.CertificateAttribute]
Field Name	Attributes
Comment	Attributes of the certificate.
Field Type	Collections.Generic.List[Crypto.Signature]
Field Name	Signatures
Comment	Signatures affixed to the certificate.
Field Type	Crypto.PrivateKeyStatus
Field Name	PrivateKeyStatus
Comment	Status of the private key. Saved as Encrypted even when Decrypted.
Field Type	Byte[]
Field Name	PrivateKeyData
Comment	Data of the private key, either encrypted or unencrypted.
Condition	PrivateKeyStatus is not Unavailable.
Field Type	Byte[]
Field Name	PrivateKeySalt
Comment	Salt used in encryption of the private key.

Condition	PrivateKeyStatus is Encrypted or Decrypted.
Field Type	Byte[]
Field Name	PassphraseSalt
Comment	Salt used to strengthen the passphrase.
Condition	PrivateKeyStatus is Encrypted or Decrypted.

Type Name	Pirate.PiVote.Crypto.CertificateAttribute
Short Name	Crypto.CertificateAttribute
Inherits	Serialization.Serializable
Comment	Attribute of a certificate.
Field Type	Crypto.CertificateAttributeName
Field Name	Name
Comment	Name of the certificate attribute.

Type Name	Pirate.PiVote.Crypto.CertificateAttribute[TValue]
Short Name	Crypto.CertificateAttribute[TValue]
Inherits	Crypto.CertificateAttribute
Comment	Attribute of a certificate.

Type Name	Pirate.PiVote.Crypto.CertificateAuthorityEntry
Short Name	Crypto.CertificateAuthorityEntry
Inherits	Serialization.Serializable
Comment	Certificate entry at a CA.
Field Type	Crypto.Secure[Crypto.SignatureRequest]
Field Name	Request
Comment	Request for signature.
Field Type	Crypto.Signed[Crypto.SignatureResponse]
Field Name	Response
Comment	Response to signature request.
Field Type	Boolean
Field Name	Revoked
Comment	Is this certificate revoked?

Type Name	Pirate.PiVote.Crypto.CertificateStorage
Short Name	Crypto.CertificateStorage
Inherits	Serialization.Serializable
Comment	Stores certificates for validation.
Field Type	Collections.Generic.List[Guid]
Field Name	RootCertificateIds
Comment	Ids of root certificates.
Field Type	Collections.Generic.List[Crypto.Certificate]
Field Name	Certificates
Comment	List of certificates.
Field Type	Collections.Generic.List[Crypto.RevocationList]
Field Name	RevocationLists
Comment	Certificate revocation lists for certificate authorities.
Field Type	Collections.Generic.List[Crypto.Signed[Crypto.RevocationList]]
Field Name	SignedRevocationLists
Comment	Signed certificate revocation lists for certificate authorities.

Type Name	Pirate.PiVote.Crypto.Encrypted
Short Name	Crypto.Encrypted
Inherits	Serialization.Serializable
Comment	Encrypted serializable object.

Field Type	Guid
Field Name	ReceiverId
Comment	Id of the intended receiver.
Field Type	Byte[]
Field Name	Data
Comment	Encrypted data of serializable object.

Type Name	Pirate.PiVote.Crypto.Encrypted[TValue]
Short Name	Crypto.Encrypted[TValue]
Inherits	Crypto.Encrypted
Comment	Encrypted serializable object.

Type Name	Pirate.PiVote.Crypto.Envelope
Short Name	Crypto.Envelope
Inherits	Serialization.Serializable
Comment	Container for a ballot.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting procedure.
Field Type	Guid
Field Name	VoterId
Comment	Id of the voter.
Field Type	Collections.Generic.List[Crypto.Ballot]
Field Name	Ballots
Comment	Casted ballot.
Field Type	DateTime
Field Name	Date
Comment	Date this envelope was formed.

Type Name	Pirate.PiVote.Crypto.Group
Short Name	Crypto.Group
Inherits	Serialization.Serializable
Comment	An group which may organize votings.
Field Type	Int32
Field Name	Id
Comment	Id of the group.
Field Type	MultiLanguageString
Field Name	Name
Comment	Name of the group.

Type Name	Pirate.PiVote.Crypto.Int32CertificateAttribute
Short Name	Crypto.Int32CertificateAttribute
Inherits	Crypto.CertificateAttribute[TValue]
Comment	Integer attribute of certificate.

Type Name	Pirate.PiVote.Crypto.NotaryCertificate
Short Name	Crypto.NotaryCertificate
Inherits	Crypto.Certificate
Comment	Certificate of a notary.
Field Type	String
Field Name	FullName
Comment	Full name of the notary.

Type Name	Pirate.PiVote.Crypto.Option
Short Name	Crypto.Option

Inherits	Serialization.Serializable
Comment	An option for which voters may vote.
Field Type	MultiLanguageString
Field Name	Text
Comment	Text of option.
Field Type	MultiLanguageString
Field Name	Description
Comment	Description of the option.
Field Type	MultiLanguageString
Field Name	Url
Comment	Url of the discussion of the option.

Type Name	Pirate.PiVote.Crypto.PartialDecipher
Short Name	Crypto.PartialDecipher
Inherits	Serialization.Serializable
Comment	A partial decipher of a vote from an authority.
Field Type	Int32
Field Name	QuestionIndex
Comment	Index of the question in question.
Field Type	Int32
Field Name	OptionIndex
Comment	Index of the option in question.
Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of the deciphering authority.
Field Type	Int32
Field Name	GroupIndex
Comment	Index of the partial decipher group.
Field Type	Emil.GMP.BigInt
Field Name	Value
Comment	Value of the partial decipher.

Type Name	Pirate.PiVote.Crypto.PartialDecipherList
Short Name	Crypto.PartialDecipherList
Inherits	Serialization.Serializable
Comment	List of partial deciphers from an authority.
Field Type	Guid
Field Name	VotingId
Comment	Id of voting procedure.
Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of issuing authority.
Field Type	Collections.Generic.List[Crypto.PartialDecipher]
Field Name	PartialDeciphers
Comment	Partial deciphers from authority.
Field Type	Int32
Field Name	EnvelopeCount
Comment	Number of envelopes that where partially deciphered.
Field Type	Byte[]
Field Name	EnvelopeHash
Comment	Hash over all envelopes that where partially deciphered.
Field Type	DateTime

Field Name	Date
Comment	Date at which the partial decipher was created.

Type Name	Pirate.PiVote.Crypto.Polynomial
Short Name	Crypto.Polynomial
Inherits	Serialization.Serializable
Comment	Integer field polynomial.
Field Type	Collections.Generic.List[Emil.GMP.BigInt]
Field Name	Coefficients
Comment	Coefficients of the polynom.

Type Name	Pirate.PiVote.Crypto.Proof
Short Name	Crypto.Proof
Inherits	Serialization.Serializable
Comment	Non-interactive zero knowledge proof that a vote sum is MaxVota.
Field Type	Emil.GMP.BigInt
Field Name	T0
Comment	Whitness.
Field Type	Int32
Field Name	C0
Comment	Challange.
Field Type	Emil.GMP.BigInt
Field Name	S0
Comment	Response.

Type Name	Pirate.PiVote.Crypto.Question
Short Name	Crypto.Question
Inherits	Serialization.Serializable
Comment	A question in a voting.
Field Type	MultiLanguageString
Field Name	Text
Comment	Text of the question.
Field Type	MultiLanguageString
Field Name	Description
Comment	Description or explaination of the question.
Field Type	MultiLanguageString
Field Name	Url
Comment	Url of the discussion of the option.
Field Type	Int32
Field Name	MaxVota
Comment	Number of vota each voter may cast.
Field Type	Collections.Generic.List[Crypto.Option]
Field Name	Options
Comment	List of possible options for the voters.

Type Name	Pirate.PiVote.Crypto.RangeProof
Short Name	Crypto.RangeProof
Inherits	Serialization.Serializable
Comment	Non-interactive zero knowledge proof that a vote is in range 0-1.
Field Type	Emil.GMP.BigInt
Field Name	T0
Comment	Witness for votum equals 0.
Field Type	Emil.GMP.BigInt
Field Name	T1

Comment	Witness for votum equals 1.
Field Type	Int32
Field Name	C
Comment	Or-Challenge.
Field Type	Int32
Field Name	C0
Comment	Challenge for vote equals 0.
Field Type	Int32
Field Name	C1
Comment	Challenge for vote equals 1.
Field Type	Emil.GMP.BigInt
Field Name	S0
Comment	Response for vote equals 0.
Field Type	Emil.GMP.BigInt
Field Name	S1
Comment	Response for vote equals 1.

Type Name	Pirate.PiVote.Crypto.RevocationList
Short Name	Crypto.RevocationList
Inherits	Serialization.Serializable
Comment	Certificate revocation list.
Field Type	Guid
Field Name	IssuerId
Comment	Id of the issuer.
Field Type	DateTime
Field Name	ValidFrom
Comment	List valid from date.
Field Type	DateTime
Field Name	ValidUntil
Comment	List valid until date.
Field Type	Collections.Generic.List[Guid]
Field Name	RevokedCertificates
Comment	List of revoked certificates.

Type Name	Pirate.PiVote.Crypto.Secure[TValue]
Short Name	Crypto.Secure[TValue]
Inherits	Crypto.Signed[TValue]
Comment	Authenticated and encrypted serializable object.

Type Name	Pirate.PiVote.Crypto.ServerCertificate
Short Name	Crypto.ServerCertificate
Inherits	Crypto.Certificate
Comment	Certificate of a voting server.
Field Type	String
Field Name	FullName
Comment	Full name of the administrator.

Type Name	Pirate.PiVote.Crypto.Share
Short Name	Crypto.Share
Inherits	Serialization.Serializable
Comment	Share from one authority given to another.
Field Type	Int32
Field Name	SourceAuthorityIndex
Comment	Index of issuing authority.

Field Type	Int32
Field Name	DestinationAuthorityIndex
Comment	Index of receiving authority.
Field Type	Emil.GMP.BigInt
Field Name	Value
Comment	Value of share.

Type Name	Pirate.PiVote.Crypto.SharePart
Short Name	Crypto.SharePart
Inherits	Serialization.Serializable
Comment	Contains all the shares and verification values of one authority.
Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of the issuing authority.
Field Type	Collections.Generic.List[Crypto.Encrypted[Crypto.Share]]
Field Name	EncryptedShares
Comment	Encrypted shares for the other authorities.
Field Type	Collections.Generic.List[Crypto.VerificationValue]
Field Name	VerificationValues
Comment	Verification values for the shares.

Type Name	Pirate.PiVote.Crypto.ShareResponse
Short Name	Crypto.ShareResponse
Inherits	Serialization.Serializable
Comment	Response of an authority to the sharings.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting procedure.
Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of the issuing authority.
Field Type	Boolean
Field Name	AcceptShares
Comment	Does the authority accept all the shares?
Field Type	Emil.GMP.BigInt
Field Name	PublicKeyPart
Comment	Public key part from that authority.
Field Type	Byte[]
Field Name	VotingParametersHash
Comment	Hash over the signed voting parameters.

Type Name	Pirate.PiVote.Crypto.Signature
Short Name	Crypto.Signature
Inherits	Serialization.Serializable
Comment	A signature to be fixed at a certificate.
Field Type	Guid
Field Name	SignerId
Comment	Certificate id of the signer.
Field Type	Byte[]
Field Name	Data
Comment	Signature data.
Field Type	DateTime
Field Name	ValidFrom

Comment	This signature is valid from then on.
Field Type	DateTime
Field Name	ValidUntil
Comment	This signature is valid until then.

Type Name	Pirate.PiVote.Crypto.SignatureRequest
Short Name	Crypto.SignatureRequest
Inherits	Serialization.Serializable
Comment	Request for a signature by a CA.
Field Type	String
Field Name	FirstName
Comment	First name of requester.
Field Type	String
Field Name	FamilyName
Comment	Family name of requester.
Field Type	String
Field Name	EmailAddress
Comment	Email address of requester.

Type Name	Pirate.PiVote.Crypto.SignatureRequest2
Short Name	Crypto.SignatureRequest2
Inherits	Crypto.SignatureRequest
Comment	Request for a signature by a CA signed by another certificate.
Field Type	Byte[]
Field Name	Signature
Comment	Signature from the signing certificate.
Field Type	Crypto.Certificate
Field Name	SigningCertificate
Comment	Signing certificate.

Type Name	Pirate.PiVote.Crypto.SignatureRequestInfo
Short Name	Crypto.SignatureRequestInfo
Inherits	Serialization.Serializable
Comment	Information that accompanies a request for a signature by a CA.
Field Type	String
Field Name	EmailAddress
Comment	Email address of requester.
Field Type	Byte[]
Field Name	EncryptedSignatureRequest
Comment	Encrypted request data.
Min Version	1

Type Name	Pirate.PiVote.Crypto.SignatureRequestSignCheck
Short Name	Crypto.SignatureRequestSignCheck
Inherits	Serialization.Serializable
Comment	Notary/authority sign check on a signature request.
Field Type	Crypto.Signed[Crypto.SignCheckCookie]
Field Name	Cookie
Comment	Signed sign check cookie from the notary/authory.
Field Type	Crypto.Certificate
Field Name	Certificate
Comment	Certificate which was signed by the notary/authority.
Field Type	DateTime

Field Name	SignDateTime
Comment	Date and time at which the sign check was created.

Type Name	Pirate.PiVote.Crypto.SignatureResponse
Short Name	Crypto.SignatureResponse
Inherits	Serialization.Serializable
Comment	Response to a signature request.
Field Type	Guid
Field Name	SubjectId
Comment	Id of the subject of this signature request response.
Field Type	Crypto.SignatureResponseStatus
Field Name	Status
Comment	Status of the signature request.
Field Type	String
Field Name	Reason
Comment	Reason the request was declined or empty.
Field Type	Crypto.Signature
Field Name	Signature
Comment	Signature of CA if accepted.

Type Name	Pirate.PiVote.Crypto.SignCheckCookie
Short Name	Crypto.SignCheckCookie
Inherits	Serialization.Serializable
Comment	Cookie authorizing the posting of sign checks.
Field Type	DateTime
Field Name	CreationDate
Comment	Data of creation of cookie.
Field Type	Byte[]
Field Name	Randomness
Comment	Random data defining the cookie.

Type Name	Pirate.PiVote.Crypto.Signed
Short Name	Crypto.Signed
Inherits	Serialization.Serializable
Comment	Signed serializable object.
Field Type	Byte[]
Field Name	Data
Comment	Binary data of serializable object.
Field Type	Byte[]
Field Name	Signature
Comment	Signature.
Field Type	Byte[]
Field Name	CertificateData
Comment	Binary data of the certificate.

Type Name	Pirate.PiVote.Crypto.Signed[TValue]
Short Name	Crypto.Signed[TValue]
Inherits	Crypto.Signed
Comment	Signed serializable object.

Type Name	Pirate.PiVote.Crypto.StringCertificateAttribute
Short Name	Crypto.StringCertificateAttribute
Inherits	Crypto.CertificateAttribute[TValue]
Comment	String attribute of certificate.

Type Name	Pirate.PiVote.Crypto.TrapDoor
Short Name	Crypto.TrapDoor
Inherits	Serialization.Serializable
Comment	A trapdoor enabled encryption of data encrypted for some certificate without the private key.
Field Type	Guid
Field Name	IssuerId
Comment	Id of the issuer of this trapdoor.
Field Type	Byte[]
Field Name	SymmetricKey
Comment	Symmetric key allowing decryption.

Type Name	Pirate.PiVote.Crypto.VerificationValue
Short Name	Crypto.VerificationValue
Inherits	Serialization.Serializable
Comment	Verification value from an authority used to check shares.
Field Type	Emil.GMP.BigInt
Field Name	Value
Comment	Value used to verify shares.
Field Type	Int32
Field Name	SourceAuthorityIndex
Comment	Index of the issuing authority.

Type Name	Pirate.PiVote.Crypto.Vote
Short Name	Crypto.Vote
Inherits	Serialization.Serializable
Comment	Elgamal encrypted vote.
Field Type	Emil.GMP.BigInt
Field Name	HalfKey
Comment	Diffie-Hellman halfkey.
Field Type	Emil.GMP.BigInt
Field Name	Ciphertext
Comment	Ciphertext.
Field Type	Emil.GMP.BigInt
Field Name	P
Comment	Prime number defining the modular arithmetic.
Field Type	Collections.Generic.List[Crypto.RangeProof]
Field Name	RangeProves
Comment	All range proves for this vote.

Type Name	Pirate.PiVote.Crypto.VoterCertificate
Short Name	Crypto.VoterCertificate
Inherits	Crypto.Certificate
Comment	Certificate for a voter.

Type Name	Pirate.PiVote.Crypto.VoteReceipt
Short Name	Crypto.VoteReceipt
Inherits	Serialization.Serializable
Comment	Receipt for a cast vote.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.

Field Type	Guid
Field Name	VoterId
Comment	Id of the voter.
Field Type	Byte[]
Field Name	SignedEnvelopeHash
Comment	Hash of the signed envelope.
Field Type	MultiLanguageString
Field Name	VotingTitle
Comment	Title of the voting.

Type Name	Pirate.PiVote.Crypto.VotingMaterial
Short Name	Crypto.VotingMaterial
Inherits	Serialization.Serializable
Comment	All things a voter needs to cast his vote.
Field Type	Crypto.Signed[Crypto.VotingParameters]
Field Name	Parameters
Comment	Defines voting procedure.
Field Type	Collections.Generic.List[Crypto.Signed[Crypto.ShareResponse]]
Field Name	PublicKeyParts
Comment	Responses that can be combined to a public key.
Field Type	Int32
Field Name	CastEnvelopeCount
Comment	Number of cast envelopes.

Type Name	Pirate.PiVote.Crypto.VotingParameters
Short Name	Crypto.VotingParameters
Inherits	Crypto.BaseParameters
Comment	Contains all parameters of a voting.
Field Type	Guid
Field Name	VotingId
Comment	Id of this voting.
Field Type	MultiLanguageString
Field Name	Title
Comment	Title of this voting.
Field Type	MultiLanguageString
Field Name	Description
Comment	Description of this voting.
Field Type	MultiLanguageString
Field Name	Url
Comment	Url of the discussion of the voting.
Field Type	DateTime
Field Name	VotingBeginDate
Comment	Date at which voting begins.
Field Type	DateTime
Field Name	VotingEndDate
Comment	Date a which voting ends.
Field Type	Int32
Field Name	GroupId
Comment	Id of the group in which the voting takes place.

Type Name	Pirate.PiVote.RemoteConfig
Short Name	RemoteConfig
Inherits	Serialization.Serializable
Comment	Config file for the voting server.

Field Type	MultiLanguageString
Field Name	SystemName
Comment	Name of the eVoting system.
Field Type	MultiLanguageString
Field Name	WelcomeMessage
Comment	Welcome message to users.
Field Type	Byte[]
Field Name	Image
Comment	Image file on the start wizard item.
Field Type	String
Field Name	Url
Comment	Url of the project.
Field Type	String
Field Name	UpdateVersion
Comment	The newest available version one could update to.
Field Type	String
Field Name	UpdateUrl
Comment	Url were one can get the update.

Type Name	Pirate.PiVote.Rpc.CreateVotingRequest
Short Name	Rpc.CreateVotingRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request creates a new voting.
Field Type	Crypto.Signed[Crypto.VotingParameters]
Field Name	VotingParameters
Comment	Parameters for the new voting.
Field Type	Collections.Generic.List[Crypto.AuthorityCertificate]
Field Name	Authorities
Comment	List of authorities to oversee the voting.

Type Name	Pirate.PiVote.Rpc.CreateVotingResponse
Short Name	Rpc.CreateVotingResponse
Inherits	Rpc.RpcResponse
Comment	Response to a voting creation RPC request.

Type Name	Pirate.PiVote.Rpc.DeleteVotingRequest
Short Name	Rpc.DeleteVotingRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request creates a new voting.
Field Type	Crypto.Signed[Rpc.DeleteVotingRequest+Command]
Field Name	Command
Comment	Signed command to delete the voting.

Type Name	Pirate.PiVote.Rpc.DeleteVotingRequest+Command
Short Name	Rpc.DeleteVotingRequest+Command
Inherits	Serialization.Serializable
Comment	Command to delete a voting.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting to delete.

Type Name	Pirate.PiVote.Rpc.DeleteVotingResponse
Short Name	Rpc.DeleteVotingResponse
Inherits	Rpc.RpcResponse

Comment	Response to a voting creation RPC request.

Type Name	Pirate.PiVote.Rpc.EchoRequest
Short Name	Rpc.EchoRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to echo.
Field Type	String
Field Name	Message
Comment	Message to echo.

Type Name	Pirate.PiVote.Rpc.EchoResponse
Short Name	Rpc.EchoResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the echo.
Field Type	String
Field Name	Message
Comment	Echoed message.

Type Name	Pirate.PiVote.Rpc.EndVotingRequest
Short Name	Rpc.EndVotingRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to end a voting procedure.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.

Type Name	Pirate.PiVote.Rpc.EndVotingResponse
Short Name	Rpc.EndVotingResponse
Inherits	Rpc.RpcResponse
Comment	Response to a request for ending a voting.

Type Name	Pirate.PiVote.Rpc.FetchAllSharesRequest
Short Name	Rpc.FetchAllSharesRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch all shares of a voting.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.

Type Name	Pirate.PiVote.Rpc.FetchAllSharesResponse
Short Name	Rpc.FetchAllSharesResponse
Inherits	Rpc.RpcResponse
Comment	Response to a request for ending a voting.
Field Type	Crypto.AllShareParts
Field Name	AllShareParts
Comment	All shares of the voting.

Type Name	Pirate.PiVote.Rpc.FetchAuthorityCertificatesRequest
Short Name	Rpc.FetchAuthorityCertificatesRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch all valid authority certificates.

Type Name	Pirate.PiVote.Rpc.FetchAuthorityCertificatesResponse
Short Name	Rpc.FetchAuthorityCertificatesResponse
Inherits	Rpc.RpcResponse

Comment	RPC response to the request to fetch all valid authority certificates.
Field Type	Collections.Generic.List[Crypto.AuthorityCertificate]
Field Name	AuthorityCertificates
Comment	List of all valid authority certificates.

Type Name	Pirate.PiVote.Rpc.FetchAuthorityListRequest
Short Name	Rpc.FetchAuthorityListRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch the list of authorities.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.

Type Name	Pirate.PiVote.Rpc.FetchAuthorityListResponse
Short Name	Rpc.FetchAuthorityListResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to a request to fetch the list of authorities.
Field Type	Crypto.AuthorityList
Field Name	AuthorityList
Comment	List of authorities for the voting.

Type Name	Pirate.PiVote.Rpc.FetchCertificateStorageRequest
Short Name	Rpc.FetchCertificateStorageRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch the certificate storage.

Type Name	Pirate.PiVote.Rpc.FetchCertificateStorageResponse
Short Name	Rpc.FetchCertificateStorageResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the certificate storage.
Field Type	Crypto.CertificateStorage
Field Name	CertificateStorage
Comment	Certificate storage from server.
Field Type	Crypto.Certificate
Field Name	ServerCertificate
Comment	Certificate of the server.

Type Name	Pirate.PiVote.Rpc.FetchConfigRequest
Short Name	Rpc.FetchConfigRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch the config.
Field Type	String
Field Name	ClientName
Comment	Name of the client software.
Min Version	1
Field Type	String
Field Name	ClientVersion
Comment	Version of the client software.
Min Version	1

Type Name	Pirate.PiVote.Rpc.FetchConfigResponse
Short Name	Rpc.FetchConfigResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the config.

Field Type	RemoteConfig
Field Name	Config
Comment	Configuration for the client.
Field Type	Collections.Generic.List[Crypto.Group]
Field Name	Groups
Comment	List of voting groups on the server.

Type Name	Pirate.PiVote.Rpc.FetchEnvelopeCountRequest
Short Name	Rpc.FetchEnvelopeCountRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	Request to fetch the number of envelopes in a voting.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.

Type Name	Pirate.PiVote.Rpc.FetchEnvelopeCountResponse
Short Name	Rpc.FetchEnvelopeCountResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the number of envelopes in the voting.
Field Type	Int32
Field Name	EnvelopeCount
Comment	Number of envelopes in the voting.

Type Name	Pirate.PiVote.Rpc.FetchEnvelopeRequest
Short Name	Rpc.FetchEnvelopeRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch an envelope.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Int32
Field Name	EnvelopeIndex
Comment	Index of the envelope.

Type Name	Pirate.PiVote.Rpc.FetchEnvelopeResponse
Short Name	Rpc.FetchEnvelopeResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering an envelope.
Field Type	Crypto.Signed[Crypto.Envelope]
Field Name	Envelope
Comment	Signed envelope.

Type Name	Pirate.PiVote.Rpc.FetchParametersRequest
Short Name	Rpc.FetchParametersRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch voting parameters.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Crypto.AuthorityCertificate
Field Name	Certificate
Comment	Certificate of the authorities.

Type Name	Pirate.PiVote.Rpc.FetchParametersResponse
Short Name	Rpc.FetchParametersResponse

Inherits	Rpc.RpcResponse
Comment	RPC response to the request to fetch voting parameters.
Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of the authority.
Field Type	Crypto.Signed[Crypto.VotingParameters]
Field Name	VotingParameters
Comment	Parameters of the voting.

Type Name	Pirate.PiVote.Rpc.FetchPartialDecipherRequest
Short Name	Rpc.FetchPartialDecipherRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch a partial decipher.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of the authority.

Type Name	Pirate.PiVote.Rpc.FetchPartialDecipherResponse
Short Name	Rpc.FetchPartialDecipherResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the partial deciphers.
Field Type	Crypto.Signed[Crypto.PartialDecipherList]
Field Name	PartialDecipherList
Comment	Signed list of partial deciphers.

Type Name	Pirate.PiVote.Rpc.FetchSignatureRequestListRequest
Short Name	Rpc.FetchSignatureRequestListRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch list signature requests.

Type Name	Pirate.PiVote.Rpc.FetchSignatureRequestListResponse
Short Name	Rpc.FetchSignatureRequestListResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering list of signature requests.
Field Type	Collections.Generic.List[Guid]
Field Name	SignatureRequestList
Comment	List of signature request ids.

Type Name	Pirate.PiVote.Rpc.FetchSignatureRequestRequest
Short Name	Rpc.FetchSignatureRequestRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch a signature request.
Field Type	Guid
Field Name	SignatureRequestId
Comment	Id of the signature request.

Type Name	Pirate.PiVote.Rpc.FetchSignatureRequestResponse
Short Name	Rpc.FetchSignatureRequestResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the signature request.
Field Type	Crypto.Secure[Crypto.SignatureRequest]

Field Name	SecureSignatureRequest
Comment	Signature request signed and encrypted for the CA.

Type Name	Pirate.PiVote.Rpc.FetchSignatureResponseRequest
Short Name	Rpc.FetchSignatureResponseRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch a signature response.
Field Type	Guid
Field Name	CertificateId
Comment	Id of the certificate.

Type Name	Pirate.PiVote.Rpc.FetchSignatureResponseResponse
Short Name	Rpc.FetchSignatureResponseResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering a signature response.
Field Type	Crypto.SignatureResponseStatus
Field Name	Status
Comment	Status of the signature response.
Field Type	Crypto.Signed[Crypto.SignatureResponse]
Field Name	SignatureResponse
Comment	Signed signature response.

Type Name	Pirate.PiVote.Rpc.FetchSignCheckCookieRequest
Short Name	Rpc.FetchSignCheckCookieRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch a signature response.
Field Type	Guid
Field Name	NotaryCertificateId
Comment	Id of the notary's or authority's certificate.
Field Type	Byte[]
Field Name	Code
Comment	Code to access the sign check cookie.

Type Name	Pirate.PiVote.Rpc.FetchSignCheckCookieResponse
Short Name	Rpc.FetchSignCheckCookieResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering a sign check cookie.
Field Type	Crypto.Signed[Crypto.SignCheckCookie]
Field Name	Cookie
Comment	Signed sign check cookie.

Type Name	Pirate.PiVote.Rpc.FetchSignCheckListRequest
Short Name	Rpc.FetchSignCheckListRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to get the list of sign checks on a certificate.
Field Type	Guid
Field Name	CertificateId
Comment	Id of the certificate.

Type Name	Pirate.PiVote.Rpc.FetchSignCheckListResponse
Short Name	Rpc.FetchSignCheckListResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering a list of sign check and the encrypted request data.
Field Type	Collections.Generic.List[Crypto.Signed[Crypto.SignatureRequestSignCheck]]

Field Name	SignChecks
Comment	List of sign checks.
Field Type	Byte[]
Field Name	EncryptedSignatureRequest
Comment	Encrypted request data.

Type Name	Pirate.PiVote.Rpc.FetchVotingMaterialVoterRequest
Short Name	Rpc.FetchVotingMaterialVoterRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch voting material and status.
Field Type	Collections.Generic.List[Guid]
Field Name	VotingIds
Comment	List of ids of the votings to get.

Type Name	Pirate.PiVote.Rpc.FetchVotingMaterialVoterResponse
Short Name	Rpc.FetchVotingMaterialVoterResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering voting material.
Field Type	Collections.Generic.List[Tuple[Crypto.VotingMaterial, Crypto.VotingStatus, Collections.Generic.List[Guid]]]
Field Name	VotingMaterials
Comment	List of tuples of voting material, status, and authorities.

Type Name	Pirate.PiVote.Rpc.FetchVotingRequest
Short Name	Rpc.FetchVotingRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to fetch voting containers.
Field Type	Collections.Generic.List[Guid]
Field Name	VotingIds
Comment	List of ids of the votings to get.

Type Name	Pirate.PiVote.Rpc.FetchVotingResponse
Short Name	Rpc.FetchVotingResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering voting containers.
Field Type	Collections.Generic.List[Rpc.VotingContainer]
Field Name	Votings
Comment	List of voting containers.

Type Name	Pirate.PiVote.Rpc.KeepAliveRequest
Short Name	Rpc.KeepAliveRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC keep alive request.

Type Name	Pirate.PiVote.Rpc.KeepAliveResponse
Short Name	Rpc.KeepAliveResponse
Inherits	Rpc.RpcResponse
Comment	RPC keep alive response.

Type Name	Pirate.PiVote.Rpc.ListVotingIdsRequest
Short Name	Rpc.ListVotingIdsRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to list voting ids.

Type Name	Pirate.PiVote.Rpc.ListVotingIdsResponse

Short Name	Rpc.ListVotingIdsResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the list of voting ids.
Field Type	Collections.Generic.List[Guid]
Field Name	VotingIds
Comment	List of voting ids.

Type Name	Pirate.PiVote.Rpc.PushCertificateStorageRequest
Short Name	Rpc.PushCertificateStorageRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to add a certificate storage to the server's data.
Field Type	Crypto.CertificateStorage
Field Name	CertificateStorage
Comment	Certificate storage to add.

Type Name	Pirate.PiVote.Rpc.PushCertificateStorageResponse
Short Name	Rpc.PushCertificateStorageResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of certificate storage.

Type Name	Pirate.PiVote.Rpc.PushEnvelopeRequest
Short Name	Rpc.PushEnvelopeRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to push an envelope.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Crypto.Signed[Crypto.Envelope]
Field Name	SignedEnvelope
Comment	Signed envelope.

Type Name	Pirate.PiVote.Rpc.PushEnvelopeResponse
Short Name	Rpc.PushEnvelopeResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of envelope.
Field Type	Crypto.Signed[Crypto.VoteReceipt]
Field Name	VoteReceipt
Comment	Receipt of the cast vote or null in case of exception.

Type Name	Pirate.PiVote.Rpc.PushPartialDecipherRequest
Short Name	Rpc.PushPartialDecipherRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to push a partial decipher.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Crypto.Signed[Crypto.PartialDecipherList]
Field Name	SignedPartialDecipherList
Comment	Signed list of partial deciphers.

Type Name	Pirate.PiVote.Rpc.PushPartialDecipherResponse
Short Name	Rpc.PushPartialDecipherResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of partial decipher.

Type Name	Pirate.PiVote.Rpc.PushShareResponseRequest
Short Name	Rpc.PushShareResponseRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to push share response.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Crypto.Signed[Crypto.ShareResponse]
Field Name	SignedShareResponse
Comment	Signed share response.

Type Name	Pirate.PiVote.Rpc.PushShareResponseResponse
Short Name	Rpc.PushShareResponseResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of share response.

Type Name	Pirate.PiVote.Rpc.PushSharesRequest
Short Name	Rpc.PushSharesRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to push share.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.
Field Type	Crypto.Signed[Crypto.SharePart]
Field Name	SignedSharePart
Comment	Signed share part.

Type Name	Pirate.PiVote.Rpc.PushSharesResponse
Short Name	Rpc.PushSharesResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of share part.

Type Name	Pirate.PiVote.Rpc.PushSignatureRequestRequest
Short Name	Rpc.PushSignatureRequestRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to push of signature request.
Field Type	Crypto.Secure[Crypto.SignatureRequest]
Field Name	SignatureRequest
Comment	Signature request signed and encrypted for the CA.
Field Type	Crypto.Secure[Crypto.SignatureRequestInfo]
Field Name	SignatureRequestInfo
Comment	Signature request signed and encrypted for the server.

Type Name	Pirate.PiVote.Rpc.PushSignatureRequestResponse
Short Name	Rpc.PushSignatureRequestResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of signature request.

Type Name	Pirate.PiVote.Rpc.PushSignatureResponseRequest
Short Name	Rpc.PushSignatureResponseRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to push signature response.
Field Type	Crypto.Signed[Crypto.SignatureResponse]

Field Name	SignatureResponse
Comment	Signed signature response.

Type Name	Pirate.PiVote.Rpc.PushSignatureResponseResponse
Short Name	Rpc.PushSignatureResponseResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to push of signature response.

Type Name	Pirate.PiVote.Rpc.PushSignCheckCookieRequest
Short Name	Rpc.PushSignCheckCookieRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request setting the sign check cookie for a notary/authority.
Field Type	Crypto.Signed[Crypto.SignCheckCookie]
Field Name	Cookie
Comment	Signed sign check cookie.

Type Name	Pirate.PiVote.Rpc.PushSignCheckCookieResponse
Short Name	Rpc.PushSignCheckCookieResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the access code to a sign check cookie.
Field Type	Byte[]
Field Name	EncryptedCode
Comment	Encrypted access code to a sign check cookie.

Type Name	Pirate.PiVote.Rpc.PushSignCheckRequest
Short Name	Rpc.PushSignCheckRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to add a sign check.
Field Type	Crypto.Signed[Crypto.SignatureRequestSignCheck]
Field Name	SignedSignCheck
Comment	Signed sign check.

Type Name	Pirate.PiVote.Rpc.PushSignCheckResponse
Short Name	Rpc.PushSignCheckResponse
Inherits	Rpc.RpcResponse
Comment	RPC response to a sign check push.

Type Name	Pirate.PiVote.Rpc.RpcMessage
Short Name	Rpc.RpcMessage
Inherits	Serialization.Serializable
Comment	Message to or from RPC server.
Field Type	Guid
Field Name	RequestId
Comment	Id of the request.

Type Name	Pirate.PiVote.Rpc.RpcRequest
Short Name	Rpc.RpcRequest
Inherits	Rpc.RpcMessage
Comment	Request message to the RPC server.

Type Name	Pirate.PiVote.Rpc.RpcRequest[TRpcServer, TResponse]
Short Name	Rpc.RpcRequest[TRpcServer, TResponse]
Inherits	Rpc.RpcRequest
Comment	Request message to the RPC server.

Type Name	Pirate.PiVote.Rpc.RpcRequest[TRpcServer]
Short Name	Rpc.RpcRequest[TRpcServer]
Inherits	Rpc.RpcMessage
Comment	Request message to the RPC server.

Type Name	Pirate.PiVote.Rpc.RpcResponse
Short Name	Rpc.RpcResponse
Inherits	Rpc.RpcMessage
Comment	RPC response message.
Field Type	PiException
Field Name	Exception
Comment	Exception throw by the RPC call if any.

Type Name	Pirate.PiVote.Rpc.VotingContainer
Short Name	Rpc.VotingContainer
Inherits	Serialization.Serializable
Comment	Container that hold all information pertaining to a voting.
Field Type	Crypto.VotingMaterial
Field Name	Material
Comment	Id of the voting.
Field Type	Collections.Generic.List[Crypto.Certificate]
Field Name	Authorities
Comment	All authorities on that voting.
Field Type	Collections.Generic.List[Guid]
Field Name	AuthoritiesDone
Comment	Authorities that are done with the current step of this voting.
Field Type	Crypto.VotingStatus
Field Name	Status
Comment	Status of the voting.
Field Type	Int32
Field Name	EnvelopeCount
Comment	Number of votes cast.

Type Name	Pirate.PiVote.Rpc.VotingStatusRequest
Short Name	Rpc.VotingStatusRequest
Inherits	Rpc.RpcRequest[TRpcServer, TResponse]
Comment	RPC request to get voting status.
Field Type	Guid
Field Name	VotingId
Comment	Id of the voting.

Type Name	Pirate.PiVote.Rpc.VotingStatusResponse
Short Name	Rpc.VotingStatusResponse
Inherits	Rpc.RpcResponse
Comment	RPC response delivering the voting status.
Field Type	Crypto.VotingStatus
Field Name	VotingStatus
Comment	Status of the voting.
Field Type	Collections.Generic.List[Guid]
Field Name	AuthoritiesDone
Comment	List of authorities that have done the current step.

Type Name	Pirate.PiVote.Serialization.Serializable
Short Name	Serialization.Serializable

Comment	Base object of all serializable objects.