Pi-Vote Protocol Documentation

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

Steinhausen, January 7, 2011, Version 1.0.7.0

Contents

1 RPC Protocol **3**
1.1 Messages 3

2 Types **3**
2.1 Basic Types 3
2.2 Enumerations 5
2.3 Objects 7

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.

2 Types

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

2.1 Basic Types

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

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

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

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

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

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

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

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

Type	System.Byte
Serialize	Just one byte

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

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

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

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

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

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

2.2 Enumerations

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

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

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

Type	Pirate.PiVote.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

Type	Pirate.PiVote.Language	
Comment	Language of the interface and texts.	
Values	English	0
	German	1
	French	2
	Italien	3

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

2.3 Objects

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

Type	Pirate.PiVote.Rpc.RpcRequest[]
Comment	Request message to the RPC server.

Type	Pirate.PiVote.Rpc.RpcRequest[,]
Comment	Request message to the RPC server.

Type	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.PartialDecipherList]
Comment	Signed serializable object.

Type	Pirate.PiVote.Rpc.PushPartialDecipherRequest
Comment	RPC request to push a partial decipher.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.
Field Type	Signed[PartialDecipherList]
Field Name	signedPartialDecipherList
Comment	Signed list of partial deciphers.

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

Type	Pirate.PiVote.Crypto.Signature
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	Pirate.PiVote.Crypto.CertificateAttribute
Comment	Attribute of a certificate.
Field Type	CertificateAttributeName
Field Name	Name
Comment	Name of the certificate attribute.

Type	Pirate.PiVote.Crypto.Certificate
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	List[CertificateAttribute]
Field Name	attributes
Comment	Attributes of the certificate.
Field Type	List[Signature]
Field Name	signatures
Comment	Signatures affixed to the certificate.
Field Type	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.
Field Type	Byte[]
Field Name	privateKeySalt
Comment	Salt used in encryption of the private key.
Field Type	Byte[]
Field Name	passphraseSalt
Comment	Salt used to strengthen the passphrase.

Type	Pirate.PiVote.Crypto.RevocationList
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	List[Guid]
Field Name	RevokedCertificates
Comment	List of revoked certificates.

Type	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.RevocationList]
Comment	Signed serializable object.

Type	Pirate.PiVote.Crypto.CertificateStorage
Comment	Stores certificates for validation.

Field Type	List[Guid]
Field Name	rootCertificateIds
Comment	Ids of root certificates.
Field Type	List[Certificate]
Field Name	certificates
Comment	List of certificates.
Field Type	List[RevocationList]
Field Name	revocationLists
Comment	Certificate revocation lists for certificate authorities.
Field Type	List[Signed[RevocationList]]
Field Name	signedRevocationLists
Comment	Signed certificate revocation lists for certificate authorities.

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

Type	Pirate.PiVote.Rpc.PushSignatureResponseResponse
Comment	RPC response to push of signature response.

Type	Pirate.PiVote.Rpc.KeepAliveRequest
Comment	RPC keep alive request.

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

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

Type	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.SharePart]
Comment	Signed serializable object.

Type	Pirate.PiVote.Rpc.PushSharesRequest
Comment	RPC request to push share.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.
Field Type	Signed[SharePart]
Field Name	signedSharePart
Comment	Signed share part.

Type	Pirate.PiVote.Rpc.PushSharesResponse
Comment	RPC response to push of share part.

Type	Pirate.PiVote.Rpc.FetchEnvelopeRequest
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	Pirate.PiVote.Rpc.FetchEnvelopeCountRequest
Comment	Request to fetch the number of envelopes in a voting.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.

Type	Pirate.PiVote.Rpc.FetchCertificateStorageRequest
Comment	RPC request to fetch the certificate storage.

Type	Pirate.PiVote.Crypto.Signed
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	Pirate.PiVote.Crypto.Signed[]
Comment	Signed serializable object.

Type	Pirate.PiVote.Crypto.VoterCertificate
Comment	Certificate for a voter.

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

Type	Pirate.PiVote.Rpc.FetchVotingMaterialVoterRequest
Comment	RPC request to fetch voting material and status.
Field Type	List[Guid]
Field Name	votingIds
Comment	List of ids of the votings to get.

Type	Pirate.PiVote.Rpc.PushSignatureRequestResponse
Comment	RPC response to push of signature request.

Type	Pirate.PiVote.Rpc.PushCertificateStorageResponse
Comment	RPC response to push of certificate storage.

Type	Pirate.PiVote.RemoteConfig
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	Pirate.PiVote.Crypto.Group
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	Pirate.PiVote.Rpc.FetchConfigResponse
Comment	RPC response delivering the config.
Field Type	RemoteConfig
Field Name	Config
Comment	Configuration for the client.
Field Type	List[Group]
Field Name	Groups
Comment	List of voting groups on the server.

Type	Pirate.PiVote.Crypto.Encrypted
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	Pirate.PiVote.Crypto.Encrypted[]
Comment	Encrypted serializable object.

Type	Pirate.PiVote.Crypto.SignatureResponse
Comment	Response to a signature request.
Field Type	Guid
Field Name	SubjectId
Comment	Id of the subject of this signature request response.
Field Type	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	Signature
Field Name	Signature
Comment	Signature of CA if accepted.

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

Type	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.VoteReceipt]
Comment	Signed serializable object.

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

Type	Pirate.PiVote.Rpc.FetchPartialDecipherRequest
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	Pirate.PiVote.Rpc.FetchSignatureResponseRequest
Comment	RPC request to fetch a signature response.
Field Type	Guid
Field Name	certificateId
Comment	Id of the certificate.

Type	Pirate.PiVote.Rpc.KeepAliveResponse
Comment	RPC keep alive response.

Type	Pirate.PiVote.Rpc.EchoRequest
Comment	RPC request to echo.
Field Type	String
Field Name	message
Comment	Message to echo.

Type	Pirate.PiVote.Crypto.Share
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	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.VotingParameters]
Comment	Signed serializable object.

Type	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.ShareResponse]
Comment	Signed serializable object.

Type	Pirate.PiVote.Crypto.VotingMaterial
Comment	All things a voter needs to cast his vote.
Field Type	Signed[VotingParameters]
Field Name	Parameters
Comment	Defines voting procedure.
Field Type	List[Signed[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	Pirate.PiVote.Rpc.FetchAuthorityListRequest
Comment	RPC request to fetch the list of authorities.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.

Type	Pirate.PiVote.Rpc.FetchSignatureRequestListRequest
Comment	RPC request to fetch list signature requests.

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

Type	Pirate.PiVote.Rpc.FetchConfigRequest
Comment	RPC request to fetch the config.

Type	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Rpc.DeleteVotingRequest+Command]
Comment	Signed serializable object.

Type	Pirate.PiVote.Rpc.DeleteVotingRequest
Comment	RPC request creates a new voting.

Field Type	Signed[Rpc.DeleteVotingRequest+Command]
Field Name	command
Comment	Signed command to delete the voting.

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

Type	Pirate.PiVote.Crypto.CertificateAttribute[]
Comment	Attribute of a certificate.

Type	Pirate.PiVote.Crypto.Int32CertificateAttribute
Comment	Integer attribute of certificate.

Type	Pirate.PiVote.Crypto.BooleanCertificateAttribute
Comment	Boolean attribute of certificate.

Type	Pirate.PiVote.Crypto.StringCertificateAttribute
Comment	String attribute of certificate.

Type	System.Tuple[Pirate.PiVote.Crypto.VotingMaterial, Pirate.PiVote.Crypto.VotingStatus, System.Collections.Generic.List[System.Guid]]
Comment	Tuple of values.

Type	Pirate.PiVote.Rpc.FetchVotingMaterialVoterResponse
Comment	RPC response delivering voting material.
Field Type	List[Tuple[VotingMaterial, VotingStatus, List[Guid]]]
Field Name	votingMaterials
Comment	List of tuples of voting material, status, and authorities.

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

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

Type	Pirate.PiVote.Rpc.FetchParametersResponse
Comment	RPC response to the request to fetch voting parameters.

Field Type	Int32
Field Name	AuthorityIndex
Comment	Index of the authority.
Field Type	Signed[VotingParameters]
Field Name	VotingParameters
Comment	Parameters of the voting.

Type	Pirate.PiVote.Rpc.FetchEnvelopeCountResponse
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	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.SignatureResponse]
Comment	Signed serializable object.

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

Type	Pirate.PiVote.Crypto.SignatureRequest
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	Pirate.PiVote.Crypto.Signed[Pirate.PiVote.Crypto.Envelope]
Comment	Signed serializable object.

Type	Pirate.PiVote.Rpc.PushEnvelopeRequest
Comment	RPC request to push an envelope.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.
Field Type	Signed[Envelope]
Field Name	signedEnvelope
Comment	Signed envelope.

Type	Pirate.PiVote.Rpc.ListVotingIdsRequest
Comment	RPC request to list voting ids.

Type	Pirate.PiVote.Rpc.FetchAllSharesRequest
Comment	RPC request to fetch all shares of a voting.
Field Type	Guid

Field Name	votingId
Comment	Id of the voting.

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

Type	Pirate.PiVote.Crypto.RangeProof
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	Pirate.PiVote.Crypto.Vote
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	List[RangeProof]
Field Name	RangeProves
Comment	All range proves for this vote.

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

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

Type	Pirate.PiVote.Rpc.FetchAuthorityCertificatesRequest
Comment	RPC request to fetch all valid authority certificates.

Type	Pirate.PiVote.Crypto.Option
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	Pirate.PiVote.Crypto.Question
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	List[Option]
Field Name	options
Comment	List of possible options for the voters.

Type	Pirate.PiVote.Crypto.SignatureRequestInfo
Comment	Information that accompanies a request for a signature by a CA.
Field Type	String
Field Name	EmailAddress
Comment	Email address of requester.

Type	Pirate.PiVote.Crypto.Proof
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	Pirate.PiVote.Crypto.Secure[Pirate.PiVote.Crypto.SignatureRequest]
Comment	Authenticated and encrypted serializable object.

Type	Pirate.PiVote.Rpc.FetchSignatureRequestResponse
Comment	RPC response delivering the signature request.
Field Type	Secure[SignatureRequest]
Field Name	SecureSignatureRequest
Comment	Signature request signed and encrypted for the CA.

Type	Pirate.PiVote.Rpc.FetchSignatureRequestRequest
Comment	RPC request to fetch a signature request.
Field Type	Guid
Field Name	signatureRequestId
Comment	Id of the signature request.

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

Type	Pirate.PiVote.Crypto.Envelope
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	List[Ballot]
Field Name	Ballots
Comment	Casted ballot.
Field Type	DateTime
Field Name	Date
Comment	Date this envelope was formed.

Type	Pirate.PiVote.Crypto.VerificationValue
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	Pirate.PiVote.Rpc.ListVotingIdsResponse
Comment	RPC response delivering the list of voting ids.
Field Type	List[Guid]
Field Name	VotingIds

Comment	List of voting ids.

Type	Pirate.PiVote.Crypto.BaseParameters
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	List[Question]
Field Name	questions
Comment	Questions in the voting.

Type	Pirate.PiVote.Rpc.CreateVotingResponse
Comment	Response to a voting creation RPC request.

Type	Pirate.PiVote.Rpc.PushPartialDecipherResponse
Comment	RPC response to push of partial decipher.

Type	Pirate.PiVote.Rpc.PushShareResponseResponse
Comment	RPC response to push of share response.

Type	Pirate.PiVote.Rpc.FetchAuthorityCertificatesResponse
Comment	RPC response to the request to fetch all valid authority certificates.
Field Type	List[AuthorityCertificate]
Field Name	AuthorityCertificates
Comment	List of all valid authority certificates.

Type	Pirate.PiVote.Rpc.PushCertificateStorageRequest
Comment	RPC request to add a certificate storage to the server's data.
Field Type	CertificateStorage
Field Name	certificateStorage
Comment	Certificate storage to add.

Type	Pirate.PiVote.Rpc.EchoResponse
Comment	RPC response delivering the echo.
Field Type	String
Field Name	Message

Comment	Echoed message.

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

Type	Pirate.PiVote.Crypto.TrapDoor
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	Pirate.PiVote.Crypto.BadShareProof
Comment	Proof of a bad sharing.
Field Type	Int32
Field Name	ComplainingAuthorityIndex
Comment	Index of the complaining authority.
Field Type	CertificateStorage
Field Name	CertificateStorage
Comment	Certificate storage.
Field Type	Signed[VotingParameters]

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

Type	Pirate.PiVote.Crypto.SignatureRequest2
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	Certificate
Field Name	SigningCertificate
Comment	Signing certificate.

Type	Pirate.PiVote.Rpc.PushShareResponseRequest
Comment	RPC request to push share response.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.
Field Type	Signed[ShareResponse]
Field Name	signedShareResponse
Comment	Signed share response.

Type	Pirate.PiVote.Crypto.Secure[Pirate.PiVote.Crypto.SignatureRequestInfo]
Comment	Authenticated and encrypted serializable object.

Type	Pirate.PiVote.Rpc.PushSignatureRequestRequest
Comment	RPC request to push of signature request.
Field Type	Secure[SignatureRequest]
Field Name	signatureRequest
Comment	Signature request signed and encrypted for the CA.
Field Type	Secure[SignatureRequestInfo]
Field Name	signatureRequestInfo
Comment	Signature request signed and encrypted for the server.

Type	Pirate.PiVote.Rpc.EndVotingResponse
Comment	Response to a request for ending a voting.

Type	Pirate.PiVote.Rpc.FetchParametersRequest
Comment	RPC request to fetch voting parameters.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.
Field Type	AuthorityCertificate
Field Name	certificate
Comment	Certificate of the authorities.

Type	Pirate.PiVote.Rpc.PushSignatureResponseRequest

Comment	RPC request to push signature response.
Field Type	Signed[SignatureResponse]
Field Name	signatureResponse
Comment	Signed signature response.

Type	Pirate.PiVote.Crypto.ShareResponse
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	Pirate.PiVote.Crypto.Secure[]
Comment	Authenticated and encrypted serializable object.

Type	Pirate.PiVote.Crypto.Polynomial
Comment	Integer field polynomial.
Field Type	List[Emil.GMP.BigInt]
Field Name	coefficients
Comment	Coefficients of the polynom.

Type	Pirate.PiVote.Rpc.CreateVotingRequest
Comment	RPC request creates a new voting.
Field Type	Signed[VotingParameters]
Field Name	votingParameters
Comment	Parameters for the new voting.
Field Type	List[AuthorityCertificate]
Field Name	authorities
Comment	List of authorities to oversee the voting.

Type	Pirate.PiVote.Crypto.Encrypted[Pirate.PiVote.Crypto.Share]
Comment	Encrypted serializable object.

Type	Pirate.PiVote.Crypto.SharePart
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	List[Encrypted[Share]]
Field Name	EncryptedShares
Comment	Encrypted shares for the other authorities.
Field Type	List[VerificationValue]
Field Name	VerificationValues

Comment	Verification values for the shares.

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

Type	Pirate.PiVote.Rpc.VotingStatusRequest
Comment	RPC request to get voting status.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.

Type	Pirate.PiVote.Rpc.EndVotingRequest
Comment	RPC request to end a voting procedure.
Field Type	Guid
Field Name	votingId
Comment	Id of the voting.

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

Type	Pirate.PiVote.Rpc.DeleteVotingResponse
Comment	Response to a voting creation RPC request.