Crosschain Interoperability Use Case

EEA Editor's Version

June 4, 2020

Editors

Weijia Zhang, PhD (Wanchain)

Sara Feenan (Clearmatics)

Peter Robinson (Consensys)

Enterprise Ethereum Alliance Crosschain Interoperability Use Cases

EEA Editor's Version June 04 , 2020

Editors:

Weijia Zhang, PhD (Wanchain)

Sara Feenan (Clearmatics)

Peter Robinson (Consensys)

Contributors to this version:

Chaals Nevile (Enterprise Ethereum Alliance), Conor Svensson (Web3Labs), Paul DiMarzio (EEA), George Ornbo (Clearmatics), Conor Svensson(Web3Labs), Jim Zhang (Kaleido), Bill Allder (EEA), Imran Bashir (JP Morgan), Jack Leahy (EEA),Brianna Rich (EEA), Brittany Mauck (EEA), John Ho (Standards Chartered), Bob Summerwill (ETC Cooperative), Sandra Johnson (Consensys), John Brainar (Consensys), Niraj Pore (Fnality), Guillaume (Atato), Antonius Leijtens (Komgo), Gorege Polzer (Everymans Ai), Johann Eid (Chainlink), Rogers Stephens (FedEx), John Brainard (Consensys), Clemens Wan (R3), Tom Willis (Intel), Izabela Czepirska (Crowdz)

Abstract

This document defines the use cases for crosschain protocols, framesworks, transactions and decentralized applications.

Status of This Document

This is a working document aiming to collect use cases and requirements for cross-chain interoperability. It does not represent consensus. It is inappropriate to cite this document other than as a work in progress.

Please send any comments to the EEA Technical Steering Committee at https://entethalliance.org/contact/.

Github Issues are preferred for discussion of this use case document.

1. Introduction

This document describes use-cases that the Enterprise Ethereum Alliance Crosschain Interoperability specification intends to address.

Crosschain interoperability broadly refers to the ability to consume data from another chain and to cause an update or another transaction on another chain.

Crosschain interoperability can take two forms:

- Homogeneous: In which two chains with similar architecture are connected (for example, two or more logically distinct EVM-based chains)
- Heterogeneos: In which two chains with different technical architecture are connected (Ethereum to the Bitcoin, for example).

Crosschain interoperability is seen as a valuable feature by both inside and out of the Enterprise Ethereum community. Users of blockchains and blockchain-inspired platforms want to make use of data and functionality on heterogenous platforms.

The goals for cross-chain interoperability specification are to:

- Describe the layers of interoperability that are relevant to Enterprise Ethereum blockchains.
- Enable data consumption between different blockchains without using a trusted intermediary.
- Allow transaction execution across blockchains without a trusted intermediary.

This use case document defines the context and scope of the crosschain interoperability specification.

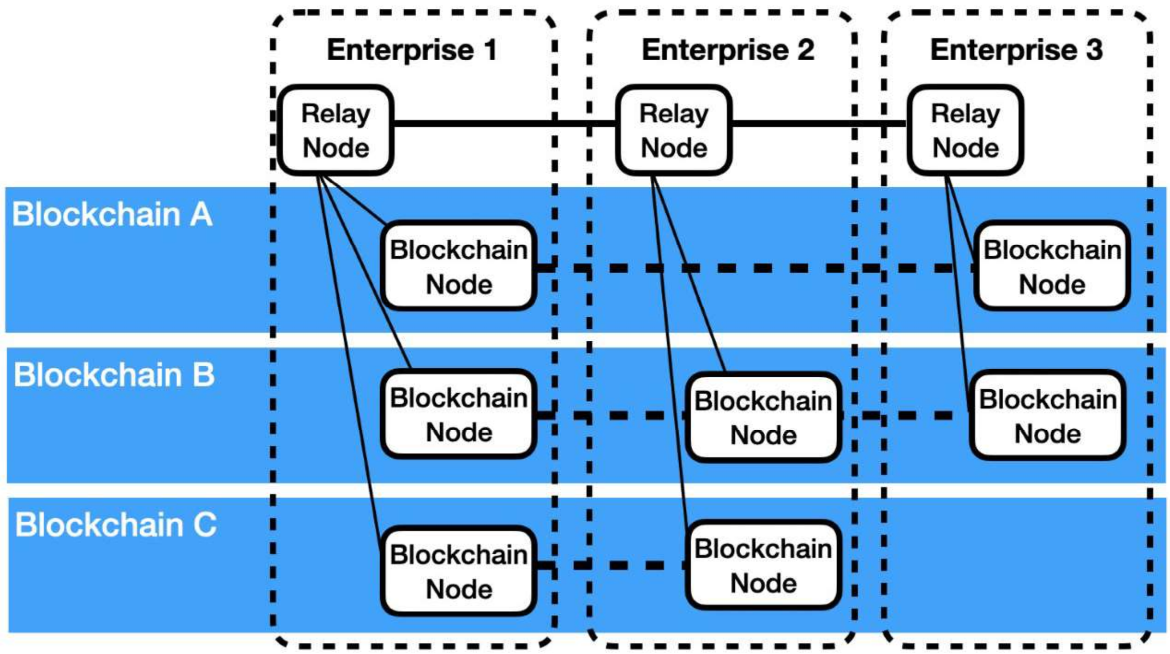
1.1 Why Produce a Crosschain Interoperability Use Case Document?

With the success of Bitcoin and Ethereum Mainnet, various blockchains such as EOS, Ripple, Litecoin, Wanchain and the like have been developed and are growing at a fast pace. There are also other private and consortium blockchains such as Hyperledger Besu, Hyperledger Fabric, Stellar, Corda, Quorum that only allow nodes with permitted identities to join the blockchain network. The growth of public and private blockchains imposes challenges for inter-chain interoperability, particularly when these chains are heterogeneous.

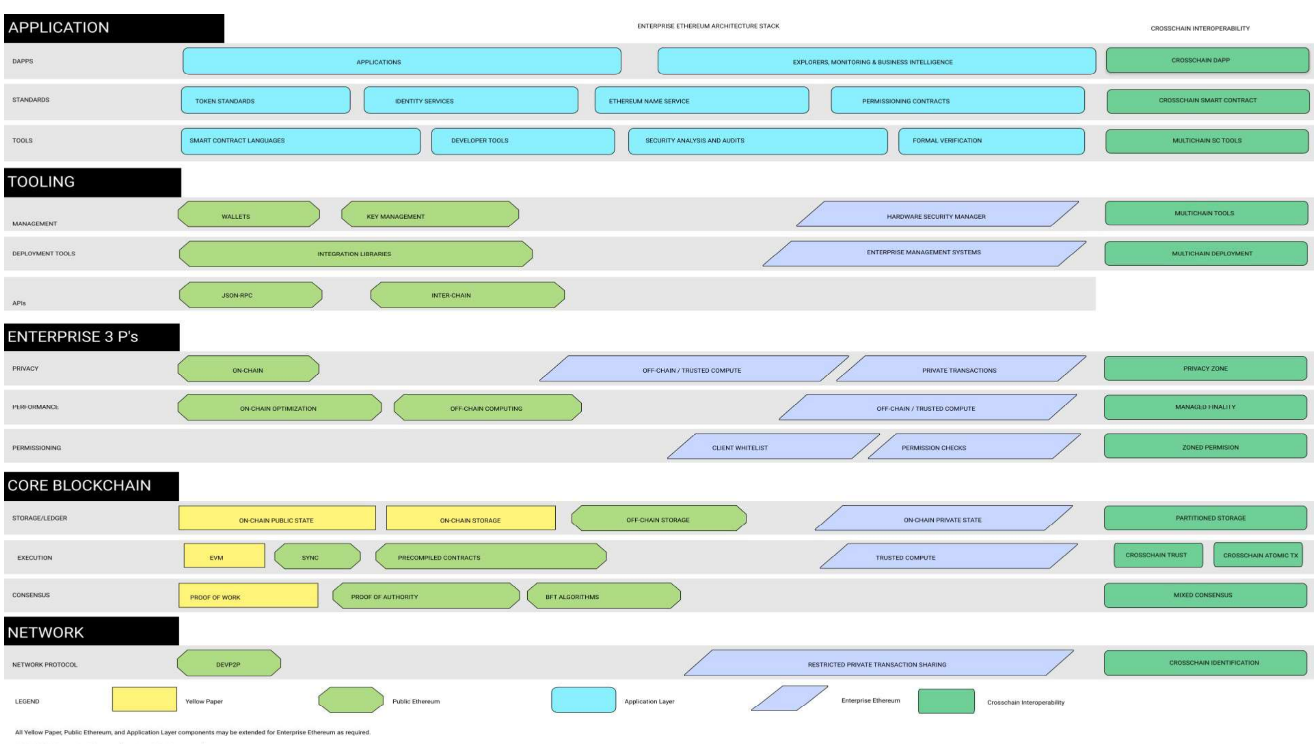
Standards-based crosschain interoperability allows enterprises to leverage the widespread knowledge of Ethereum in blockchain development. This use case document defines the scope of problems for crosschain interoperability specification to tackle.

2. Crosschain Interoperability Architectural Schematic Diagram

Diagram showing routing nodes connecting three blockchains that are hosted between three companies.



The following diagrams show the crosschain interoperability architectural components.



In the above diagram, the crosschain interoperability components added to the existing Enterprise Ethereum architecture are grouped in a column on the right hand side and explained below:

For the application layer, there are three main components: Crosschain app, Crosschain smart contract, multichain smart contract tools.

Crosschain apps provide end users with interfaces to connect to multiple blockchains and enable them to do cross-chain transactions

Crosschain Smart Contracts are deployed to a source blockchain, a target blockchain, and any bridging blockchain to allow transactions, events, messages, and assets to atomically flow from one blockchain to another.

Multichain Smart Contract Tools enable a user to interact with smart contracts in various blockchains from a single console.

For the tooling layer, crosschain interoperability components may contain multichain tools such as multichain wallet and browser. Multichain Tools provide utilities and tooling to enable connections to multiple blockchains from a single client or user interface.

Multichain deployment tools provide a single console to compile, deploy, and test smart contracts on the corresponding blockchain from a single application.

For the Enterprise 3P layer, the crosschain interoperability components can include privacy zones, managed privacy, and zoned permission.

Privacy zones group different blockchains and blockchain nodes based on privacy requirements and only allow access to clusters with the same privacy setting.

Zoned permission sets access right of blockchain nodes based on geographical locations.

For the core blockchain layer, the crosschain interoperability can comprise partitioned storage, crosschain trust, crosschain atomic transactions, and mixed consensus.

Partitioned storage divides blockchain data sets into various chucks and restricts crosschain access for some blockchain storage.

Crosschain trust provides a mechanism for one blockchain to trust the signature and proof from another blockchain and allows direct crosschain operations.

Crosschain atomic transactions ensure crosschain transactionw must be either committed or revoked, prohibiting an unresolved transaction that impair the integrity of blockchains.

Mixed consensus allows a crosschain transaction to go through two blockchains with different consensus.

For the blockchain network layer, crosschain interoperability can include crosschain identification.

Crosschain identification provides specification for blockchain identification, characterization, and discovery.

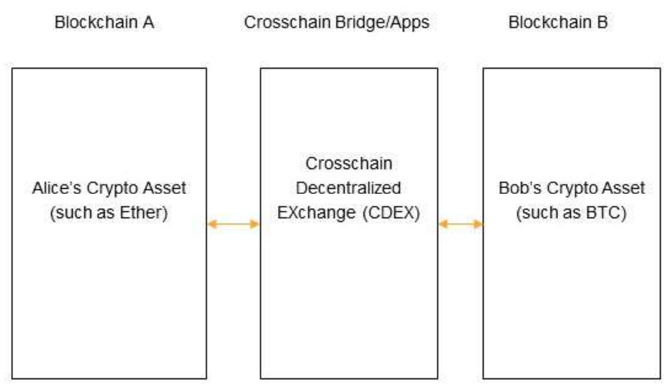
The following diagrams show the crosschain interoperability architectural components and use case relationships

Components \ Usecases	Crosschain Decentralized Exchange	Crosschain Asset Trading	Crosschain Asset Transform	Crosschain Backup	Blockchain based Key Management	Crosschain Information Syndication	Crosschain Gas Swap	Selective Transparency and Privacy	Crosschain Supplychain	Crosschain with Soverign Data	Crosschain Oracle	Crosschain Charity
Crosschain Dapp	Add On	Add On	Add On	Add On	Add On	Add On	Add On	Add On	Add On	Add On	Add On	Add On
Crosschain Smart Contract	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required
Multichain SC Tools	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend
Multichain Tools	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend
Multichain Deployment	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend	Recommend
Privacy Zone	Optional	Optional	Optional	NA	Recommend	Optional	Optional	Required	Recommend	Required	Recommend	Optional
Managed Finality	Required	Required	Required	Recommend	Recommend	Optional	Required	Recommend	Required	Recommend	Optional	Optional
Zoned Permission	Optional	Optional	Optional	Optional	Optional	Optional	NA	Required	Recommend	Required	Optional	Optional
Partitioned Storage	Optional	Optional	Optional	Optional	Optional	Optional	Optional	Required	Optional	Required	Optional	Optional
Crosschain Trust	Required	Required	Required	Recommend	Required	Optional	Required	Required	Required	Required	Required	Required
Crosschain Atomic TX	Required	Required	Required	Optional	Required	Optional	Required	Required	Required	Required	Required	Required
Mixed Consensus	Recommend	Recommend	Recommend	NA	Recommend	NA	NA	Recommend	Recommend	Recommend	NA	Recommend
Crosschain Identification	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required	Required

3. Crosschain Interoperability Use Cases

3.1 Crosschain Decentralized Exchange

Crosschain Decentralized Exchange (CDEX) is a system that allows cryptocurrencies to be exchanged across different blockchains. For example, after selling a cryptokitty to Bob, Alice now has some bitcoin. Later Alice decides to convert the bitcoin to ether. Alice then uses her crosschain wallet to send an exchange order. She specifies the target currency, the desired exchange rate, and the address to receive the ether. Bob has some ether and would like to exchange it for bitcoin. Bob sees Alice's sell order and accepts the sell price. The bitcoin specified in Alice'ssell order is then transferred to Bob's address, and a corresponding amount of Bob's ether is then transferred to Alice's address. If there is any failure, the exchange operation is cancelled. There are several situations to consider: for example, Alice or Bob might exchange the asset in part or in whole; they can also specify the expiration date for the exchange order.

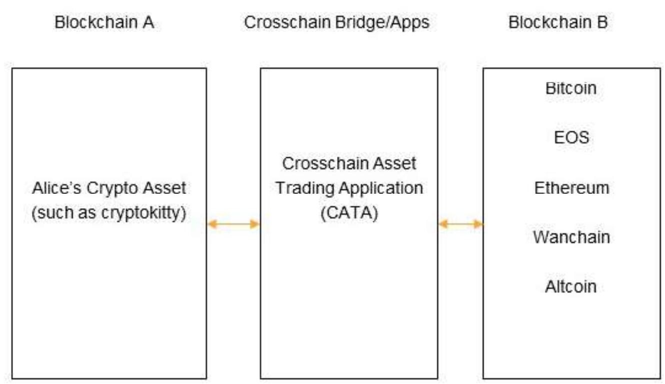


Use case: Crosschain Decentralized EXchange (CDEX)

3.2 Crosschain Asset Trading Applications

Crosschain Asset Trading Application (CATA) is a system that allows a user to sell crypto assets to another user with accounts on any supported blockchain. For example, Alice has a cryptokitty asset on the Ethereum blockchain and wants to sell the asset to another user. Alice has accounts on other blockchains such as Bitcoin, EOS, Wanchain, etc., and is open to accepting offers from other blockchains. The CATA system has multi-chain support so that it can communicate with the original chain (Blockchain A) and an external chain (blockchain B) with operations such as querying block and event information, sending transactions, etc. The CATA system also has access to an oracle to access crypto exchange rates.

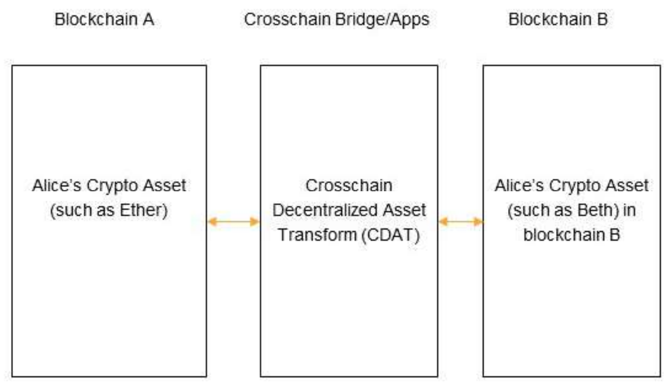
To place a sell order, Alice connects to CATA using a wallet and specifies the asset to sell, target price, the acceptable type of currency, and the account address to receive payment for each blockchain. CATA then checks if the specified crypto currency is among the supported blockchains. If yes, the CATA system will retrieve the exchange rate between the original and external blockchain and calculate the target sale prices of Alice’s asset denominated in various specified assets on other blockchains. CATA then publishes Alice’s sell order to an order book so that any user with a CATA wallet can access it. CATA user Bob sees Alice’s Sell Order and decides to purchase the cryptokitty asset from Alice. Bob does not have an Ethereum account but does have a Bitcoin account and his balance is sufficient to purchase the cryptokitty. Using the CATA wallet’s crosschain operation feature, Bob creates an account on the Ethereum blockchain. Then using CATA’s query feature, Bob remotely queries the exchange rate of bitcoin and ether and figures out the real time sale price of the cryptokitty asset in bitcoin. Bob then submits a crosschain transaction to perform an atomic transaction across the Bitcoin and Ethereum blockchains. Once the transaction is completed, Bob’s cryptocurrency is transferred into Alice’s Bitcoin account and Alice’s cryptokitty ownership is transferred to Bob's Ethereum account.



Use case: Crosschain asset trading application (CATA)

3.3 Crosschain Decentralized Asset Transform

The Crosschain decentralized asset transform (CDAT) system allows a crypto asset on one blockchain to be transformed to another format of asset on the same or different blockchain while maintaining its original value. The transformed asset can be used in the new chain to take advantage of the new asset format, and the performance and scalability of the new chain. For example, EthGame has a decentralized application that allows any ERC20 token to be used. Bob wants to play the games in EthGame, but he only has Bitcoins. EthGame then builds a smart contract and crosschain service to allow Bob to lock certain amount of BTC on the Bitcoin blockchain, and the same amount of an ERC20 mapping token (such as wbtc_erc20) that represents bitcoin is generated and assigned to Bob's address on Ethereum. Bob can then use his wbtc_erc20 token to play in EthGame to trade with other ERC20 tokens or ether. Bob can also redeem wbtc_erc20 back to bitcoin at any time.



Use case: Crosschain Decentralized Asset Transform (CDAT)

3.4 Crosschain Backup

For public blockchains, normally there are many nodes running the same program and same data storage and therefore data redundancy is not a concern. For private or consortium blockchains, there is a limited amount of nodes running on one blockchain and some users may want to back up some block or transaction data to another blockchain. For example, a user may specify a chuck of data, a block number, or a transaction hash and request to save the data to another blockchain. The other blockchain will return a hash or a reference to show where the data is saved. The backup blockchain can also provide a service showing what backup transactions have been requested and completed. Also, for two organizations doing business with their own blockchains, there is a need for each blockchain to have a backup data for the other blockchain.

3.5 Using a Private Chain for Key Management

In this use case, there is a private blockchain connected to multiple public blockchains. The private blockchain is secured and trusted and users use the private blockchain to do the following operations:

- Use a client to connect to the private blockchain
- Create accounts for a public blockchains from the private blockchain
- Sign transactions and messages in the private blockchain and send the information to the intended public blockchains
- Support multisign so that multiple accounts in the private blockchain can sign a transaction together for public blockchains.

One usage scenario is for an organization to have a private blockchain to manage working accounts for public blockchains. Instead of creating and connecting wallets to every public chain through attach or rpc connections, crypto wallets are only connected to the private blockchain and use it as the proxy to access other public blockchain to ensure security.

3.6 Crosschain Information Syndication

Crosschain information syndication allows one blockchain to refer to assets, events, properties, or data in another blockchain. In order for a source blockchain to list assets in various external blockchains, it can use links to refer to entities in other blockchains. For example, a smart contract in blockchain A can refer to an address in blockchain B as chain-id-b/addresss where chain-id-b is the chainid for blockchain B.

3.7 Crosschain Ether Swap for Gas Trading

Two or more private Ethereum blockchains may charge gas as a method of controlling the rate that consortium members submit transactions to the blockchains. An entity may have additional Ether on one blockchain, and may need to send more transactions on another blockchain. The entity could execute an atomic swap of Ether between blockchains, thus allowing them to have more Ether on the chain they wish to execute more transactions on.

3.8 Selective Transparency with Selective Privacy

In this use case there are three blockchains:

- A supply chain blockchain that has all the information related to a supply chain. The membership of this chain is strictly limited to the members of the supply chain consortium.
- A regulatory blockchain that has most of the members of the supply chain, plus a government regulator. The information published to this chain is information required for compliance reasons, but does not include the details in the supply chain blockchain.
- A customer blockchain that holds information that gives customers assurance of the provenance of the goods they are purchasing.

An atomic crosschain transaction would allow events in the supply chain blockchain to be selectively published to the regulatory blockchain and the customer blockchain. This would allow for selective privacy with selective transparency. Atomic behaviour is required to ensure events that should be reflected in the regulatory or customer blockchain don't appear solely in the supply chain blockchain (or just in the customer or regulatory blockchains) due to a failure.

This requires atomic crosschain transactions that can call across multiple blockchains as a result of a single application transaction.

3.9 Logistics and Finance Blockchain Communications

In this use case there are two blockchains:

- Logistics blockchain that tracks physical shipments of goods.
- Finance blockchain that is used for financial transactions.

When an item is marked as "delivered" (probably involving a bill of lading) on the logistics blockchain, the finance blockchain should be updated to transfer money based on delivery.

This requires atomic Crosschain Transactions that update state on one blockchain based on a function call on another blockchain.

For two consortiums doing business, they could each have a private blockchain. Allowing for permissioning, the two private blockchains need to be able to read values from the other blockchain and do atomic crosschain transactions.

3.10 Nation State Sovereign Data

A nation state may pass a law forbidding certain information leaving the countries borders. This could require all blockchain nodes be inside the country. In this case, there would be blockchains within the country, and blockchains outside the country. Crosschain transactions are needed to allow the blockchains inside the country to interact with blockchains outside the country.

3.11 Oracle Chain

An "Oracle" blockchain could hold information such as exchange rates or other information. The maintainer of the permissioned blockchain may charge for access to the blockchain. The maintainer of the blockchain could allow other blockchains to execute crosschain function calls that read data from the Oracle blockchain.

For example, a contract to buy goods may be in a certain currency. The Oracle contract would be used when executing the deal in the contract to determine how much blockchain native currency should be exchanged, based on the currency.

3.12 Crosschain Charity

In this scenario, Alice is a representative of a charity organization and is organizing a charity drive. Alice set up an account in one blockchain and deployed smart contract to receive the donation. Conventionally, Alice can only receive donations for crypto assets on the same blockchain. With crosschain capability, Alice can extend the supported donation to other blockchains. For donor Bob who does not have a crypto account in the blockchain where Alice deployed the charity smart contract, he can use crosschain to donate directly to Alice’s charity account without the need of going through an exchange to convert and transfer assets through a third party.

A. Acknowledgments

The EEA acknowledges and thanks the many people who contributed to the development of this version of the specification. Please advise us of any errors or omissions.

Enterprise Ethereum is built on top of Ethereum, and we grateful to the entire community who develops Ethereum, for their work and their ongoing collaboration to helps us maintain as much compatibility as possible with the Ethereum ecosystem.

B. References

B.1 Informative references

Enterprise Ethereum Alliance Implementation Guide V5.0. Enterprise Ethereum Alliance, Inc.

C. Legal Notice

The copyright in this document is owned by Enterprise Ethereum Alliance Inc. ("EEA" or "Enterprise Ethereum Alliance"). This document shall be used for information purposes only. Use of this document and any related intellectual property incorporated herein, is also governed by the Bylaws, Intellectual Property Rights Policy and other governing documents and policies of EEA and is subject to the disclaimers and limitations described below.
THE CONTENTS OF THIS DOCUMENT ARE PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE. EEA DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY.
NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE APPLICABILITY OR NON-APPLICABILITY OF ANY REGULATORY CONTROLS OR COMPLIANCE WITH ANY LAWS OR REGULATIONS IN ANY JURISDICTION. No regulatory authority has examined or approved any of the information set out in this document. No such action has been or will be taken under the laws, regulatory requirements, or rules of any jurisdiction. The publication, distribution or dissemination of this document does not imply that the applicable laws, regulatory requirements, or rules have been complied. In no event should the content of this document be interpreted or used as, or relied upon, as legal, compliance, regulatory or other professional advice.
EEA has not investigated or made an independent determination regarding title or non-infringement of any technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, Standards, and specifications, including through the payment of any required license fees. NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT. IN NO EVENT SHALL EEA OR ANY OF ITS MEMBERS BE LIABLE TO THE USER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT