Appendix – Risk and Threat Analysis of the BlockVoke/ACME Extension

The detailed descriptions of the assets identified as part of the risk and threat analysis of BlockVoke are given in Tables 1-6, and the risk and threat analysis for the risks identified in the BlockVoke/ACME Extension is given in Tables 7-15.

Table 1: ACME Validation Challenge asset identification

Business asset	**ACME Challenge Object**
IS assets	Send ACME Validation Challenge, Receive ACME Validation Challenge
Process description	**Send ACME Validation Challenge** 1. ACME CA Sends ACME Validation Challenge object to CO. **Receive ACME Validation Challenge** 1. CO Receives ACME Validation Challenge object from CA.
Security Criteria	**Send ACME Validation Challenge**, **Receive ACME Validation Challenge**: Securely, with integrity and availability.

Table 2: ACME Validation Response asset identification

Business asset	**ACME Response** Object
IS assets	Send ACME Validation Response, Receive ACME Validation Response
Process description	**Send ACME Validation Response** 1. CO sends ACME Response object to the CA. **Receive ACME Validation Response** 1. ACME CA receives and validates ACME challenge object.
Security Criteria	**Send ACME Validation Response**, **Receive ACME Validation Response**: Securely, with integrity and availability.

Table 3: ACME Account asset identification

Business asset	**ACME Account** Object: including CO's Contact Information, CO's ACME KeyPair
IS assets	Send ACME Order, Receive ACME Order, Send ACME Revocation Request, Receive ACME Revocation Request
Process description	**Send ACME Order** 1. CO uses their ACME private key to sign their new ACME Order. 2. CO sends the newly signed ACME Order. **Receive ACME Order** 1. ACME CA recieves the signed ACME Order. 2. ACME CA verifies the signature using their copy of the CO's public key.
Security Criteria	**Send ACME Order**, **Receive ACME Order**: Securely, with integrity and availability.

Table 4: CSR asset identification

Business asset	**CSR**
IS assets	Send CSR to CA
Process description	**Send CSR to CA** 1. CO sends CSR to the ACME CA. 2. CA verifies the CO's signature in CSR
Security Criteria	**Send CSR to CA**: Securely, with integrity and availability.

Table 5: Certificate asset identification

Business asset	**Certificate**
IS assets	Certificate Generation, Certificate Sending, Certificate Receiving, Certificate Verification, Mark Certificate as Revoked
Process description	**Certificate Generation** 1. CA generates a 1-of-2 multisignature address using CSR and their own generated bitcoin address. 2. CA adds the multisignature address as an extension field of the certificate. 3. CA adds their signature to the certificate. **Certificate Sending** 1. The CO/CA sends a copy of the certificate to end–user. **Certificate Receiving** 1. Certificate is Received by an end–user. **Certificate Verification** 1. Certificate fingerprint is verified by the end–user. 2. End–user verifies the certificate signature using the CA's public key. **Mark Certificate as Revoked** 1. End–user checks Mempool/checks Blocks and finds a TX:Revoke transaction. 2. End–user marks certificate as revoked based on `OP_RETURN` script.
Security Criteria	**Certificate Generation**, **Certificate Verification**, **Mark Certificate as Revoked** : Securely, with integrity **Certificate Sending**, **Certificate Receiving** : Securely, with integrity and availability

Table 6: Transaction Asset Identification

Business asset	Transaction (Tx:Fund/Tx:Revoke transactions)
IS assets	Transaction Sending
Process description	**Transaction Sending** 1. Revoking party sends revocation transactions to the Bitcoin blockchain network.
Security Criteria	**Transaction Sending**: Availability, with Integrity.

Table 7: Risk and Threat analysis for *ACME Validation Challenge/Response Modified*

Threat Agent	Outside Man-In-The-Middle (MITM) attacker. Motivation: Undermine the trustworthiness and reliability between the ACME CA and CO, and hence the ACME validation of the CO's Bitcoin address public key. Resources: Intercept traffic between the CO and the CA. Expertise: Intercept and manipulate the ACME Validation challenges or responses being sent by the CO; more specifically targeting the validation of the CO's Bitcoin address public key.
Attack Method	1. The outside attacker intercepts the ACME validation challenges requested by the CO or responses sent by the CO. 2. The outside attacker manipulates the ACME validation challenges/responses. 3. The outside attacker forwards the manipulated ACME validation challenges/responses to the CO or CA respectively.
Threat	Outside attacker can forward manipulated ACME validation challenges/responses to the CO or CA respectively.
Vulnerability	ACME validation challenges/responses; can be intercepted while being transmitted.
Event	Outside attacker manipulates transmitted ACME validation challenges/responses and forwards them to the CO/CA respectively.
Impact	1. The outisde attacker intercepts manipulates the ACME validation challenges/responses; thereby invalidating them, undermining the trust between the CO and the CA.
Risk	Outside attacker manipulates transmitted ACME validation challenges/respones and prevents ACME validaion process, and thereby the certificate generation process.

Table 8: Risk and Threat analysis for *ACME Validation DDoS*

Threat Agent	Outside attacker (DDoS). Motivation: Undermine the reliability of the network between the ACME CA and CO, and hence the ACME validation of the CO's Bitcoin address public key. Resources: Distributed network of devices used maliciously to clog the network used for the ACME validation process between the CO and the CA. Expertise: To be able to clog the bandwidth of the ACME CA.
Attack Method	1. The outside attacker identifies, and gains access to the network used by the ACME CA for ACME Validation process. 2. The outside attacker establishes a network of distributed malicious devices that are capable of interacting with the network. 3. The outside attacker used these devices to maliciously clog the available bandwidth of the ACME CA server.
Threat	Outside attacker can deny the ACME Validation process from proceeding.
Vulnerability	ACME CA server is not adequately pretected against DDoS attacks.
Event	Outside denies ACME Validation process from proceeding by clogging the ACME CA's netwokr bandwidth.
Impact	1. ACME CA's network bandwidth is clogged. 2. ACME validation process, among other ACME processes cannot proceed.
Risk	Outside attacker can deny ACME Validation processes, among other ACME processes by a DDoS attack on the ACME CA.

Table 9: Risk and Threat analysis for *Malicious CO*

Threat Agent	Malicious CO Motivation: Remote Code Execution (RCE) on an ACME CA's device, to produce a certificate that cannot be revoked using the generated multisignature address, and undermine trustworthiness in the BlockVoke revocation process. Resources: Knowledge about ACME CA's multisignature address generation software. Expertise: Modify the Bitcoin public key attribute of the CSR to enable RCE during the CA's multisignature address creation process, or generation of a multisignature address un–revocable using the BlockVoke protocol.
Attack Method	1. The malicious CO inserts invalid data or malicious code into the CO's Bitcoin public key attribute in the CSR. 2. CA attempts to create multisignature address using the malicious CO Bitcoin public key leading to an invalid multisignature address or an RCE on the CA's device.
Threat	Malicious CO inserts invalid data or code in the place of the Bitcoin address public key to the CA in the CSR.
Vulnerability	CA does not check the validity of the CO's Bitcoin address public key before generating the multisignature address.
Event	Malicious CO sends invalid data or code in the place of the Bitcoin address public key to the CA in the CSR, which is not checked for validity by the CA and leads to an invalid multisignature address or an RCE.
Impact	Invalid multisignature address, or an RCE attack on the CA's device.
Risk	Malicious CO exploits a CA that does not validate CSR's Bitcoin address public key attribute and is able to force generation of an invalid multisignature address or an RCE on the CA's device.

Table 10: Risk and Threat analysis for *Malicious CA*

Threat Agent	Malicious CA Motivation: Generate a certificate that is not revocable using BlockVoke. Resources: Creating invalid multisignature addresses. Expertise: Manipulate the multisignature address attribute of the certificate to enable an irrevocable certificate to be created and accepted by end–user's organization.
Attack Method	1. The malicious CA adds an invalid multisignature address to the certificate attribute field. 2. End–user's organization accepts certificate.
Threat	Malicious CA generates a certificate un–revocable using the BlockVoke protocol, that end–user's organization accepts.
Vulnerability	Members of the end–user's organization do not check multisignature address of certificate before accepting the certificate.
Event	Malicious CA uses an invalid multisignature address in the generated certificate. End–users accept the certificate without validation of the multisignature address, leading to certificate to be accepted that is un–revocable using the BlockVoke protocol.
Impact	Creation and acceptance of an un–revocable certificate.
Risk	Malicious CA creates a certificate un–revocable using BlockVoke protocol by exploiting the vulnerability of end–users not validating the multisignature address.

Table 11: Risk and Threat analysis for *Certificate Modified*

Threat Agent	Outside Attacker (MITM) Motivation: Undermine the trustworthiness and reliability in certificate sending/receiving processes. Resources: Intercepted traffic between the CO/CA and end–users. Expertise: Intercept and manipulate the traffic between the CA/CO and members of the end–user's organization.
Attack Method	1. The outside attacker intercepts the certificate being sent by a CO/CA to the end–user's organization. 2. The outside attacker manipulates the certificate. 3. The outside attacker forwards the manipulated certificate to the end–user's organization.
Threat	Outside attacker forwards a manipulated certificate to the end–user's organization.
Vulnerability	New certificates can be manipulated while being transmitted.
Event	Outside attacker intercepts and manipulates transmitted certificate and sends it to the end–user's organization.
Impact	Members of the end–user's organization fail to verify the CA's signature in the certificate and do not trust the certificate.
Risk	Outside attacker manipulates transmitted certificate and prevents certificate verification.

Table 12: Risk and Threat analysis for *Certificate DDoS*

Threat Agent	Outside Attacker (DDoS) Motivation: Undermine the reliability in certificate sending/receiving processes. Resources: Distributed network of malicious devices capable of clogging the network used for certificate sending/receiving. Expertise: Clog the communication network used for the certificate sending/receiving processes using a distributed network of malicious devices.
Attack Method	1. The outside attacker identifies the communication network used by the CA/CO to send new certificates to the end–user's organization. 2. The outside attacker establishes a network of distributed malicious devices that can interact within the communication network. 3. The outside attacker uses the network of distributed malicious devices to clog the bandwidth of the communication network.
Threat	Outside attacker can deny certificate sending/receiving processes.
Vulnerability	Communication network used for the certificate sending/receiving processes is not protected from DDoS attacks from malicious attackers with access to that network.
Event	Outside attacker denies the communication of the new certificates to the end–user.
Impact	1. Certificate communication network bandwidth is clogged 2. New certificates cannot be sent to end–user's organization for verification.
Risk	Outside attacker can prevent new certificates from being sent to the end–user's organization by perpetrating a DDoS attack on the communication network.

Table 13: Risk and Threat analysis for *Transaction Modified*

Threat Agent	Malicious Attacker Motivation: Undermine reliability of the certificate revocation process. Resources: Knowledge and access to the network used by the CO/CA to send revocation transactions. Expertise: Intercept transactions before a CO/CA transmits them to the blockchain network.
Attack Method	1. The outside attacker intercepts a revocation transaction from a CA/CO before it is transmitted to the blockchain network. 2. The outside attacker manipulates the transaction, making it invalid or discards it.
Threat	Outside attacker can undermine reliability of certificate revocation by manipulating transactions, making them invalid or discard them.
Vulnerability	CO/CA initiating the revocation uses an insecure communication method that allows transactions to be intercepted.
Event	Outside attacker intercepts and manipulates or discards a certificate revocation transaction.
Impact	1. Certificate revocation transactions are rendered invalid or discarded by the blockchain network, leading to the certificate not being revoked using the BlockVoke protocol.
Risk	Outside attacker manipulates or discards the revocation transaction, disabling the certificate from being revoked.

Table 14: Risk and Threat analysis for *End–User new revocations modified*

Threat Agent	Outside Attacker (MITM) Motivation: Revoke certificates that have not been revoked or prevent the rest of the End–User's organisation to know about new revocations or CRLite filter updates. Resources: Knowledge of the communication system used by the end–user to communicate new revocations to their organisation. Expertise: Intercept new revocations from the end–user to the rest of their organisation and modify or add to them as they please.
Attack Method	1. The outside attacker intercepts the certificate being sent by a CO/CA to an end–user. 2. The outside attacker modifies or adds new revocations to the CRLite filter and communicates the modified revocations to the end–user's organisation.
Threat	Outside attacker can modify revocations or add new revocations to the communication system used between the end–user and their organisation.
Vulnerability	Communication system used by the end–user to communicate new revocations to their organisation is not authenticated.
Event	Outside attacker intercepts and modifies revocations being sent from the end–user and their organisation.
Impact	1. End–user's organisation trusts certificates that are possibly compromised. 2. End–user's organisation marks some certificates as revoked that were not actually revoked, causing a disruption to certain certificate reliant systems.
Risk	Tamper-susceptible communication system between the end–user and their organisation allows an outside attacker to prevent end–user's organisation to know about new revocations or revoke certificates that otherwise have not been revoked.

Table 15: Risk and Threat analysis for *End–User new revocations DDoS*

Threat Agent	Outside Attacker (MITM) Motivation: Prevent the rest of the End–User's organisation such as clients/employees to know about new revocations/CRLite filter updates. Resources: Distributed network of malicious devices with the capability of clogging the network used by the end–user to communicate new revocations to their organisation. Expertise: Clog the communication medium used by the End–User to communicate new revocation information to the rest of their organisation using a distributed network of malicious devices.
Attack Method	1. The outside attacker identifies the network used by the end–user to communicate new revocations or updates to CRLite filter to the rest of their organisation. 2. The outside attacker establishes a network of distributed devices. 3. The outside attacker uses the network of distributed devices to clog the bandwidth of the communication network.
Threat	Outside attacker can undermine the certificate revocation process by preventing the end–user's organisation from knowing about new revocations.
Vulnerability	Communication medium used for new revocations or CRLite filter updates is vulnerable to DDoS attacks.
Event	Outside attacker denies new revocations from being communicated to end–users's organisation.
Impact	End–user's organisation or employees are not aware of new revocations and trusts possibly compromised certificates.
Risk	An outside attacker can deny new revocation information to be communicated to end–users by a DDoS attack on the underlying communication network.