Threat Modeling Report

Created on 11/15/2020 3:52:53 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	15
Needs Investigation	0
Mitigation Implemented	17
Total	32
Total Migrated	0

Diagram: Diagram 1

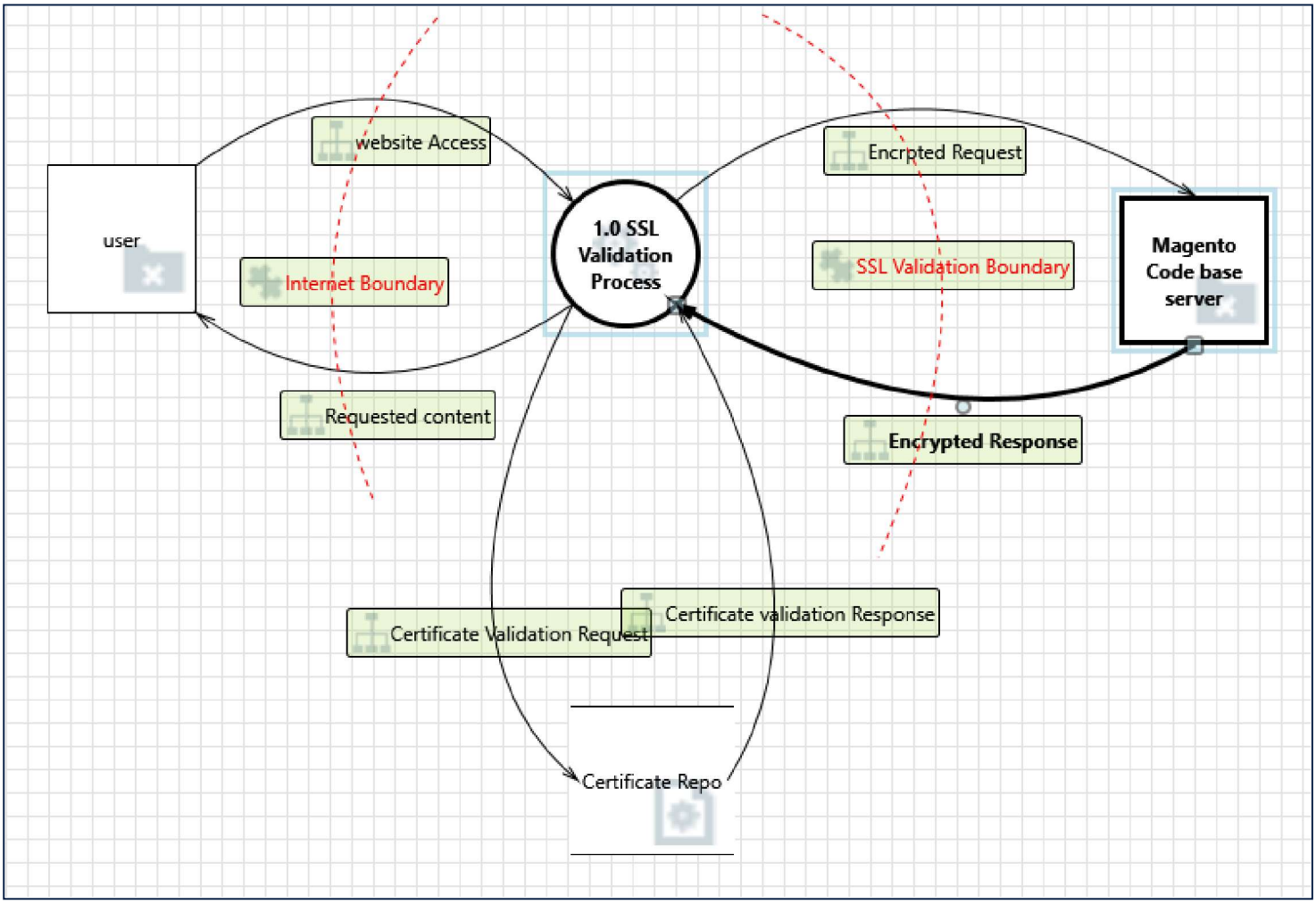
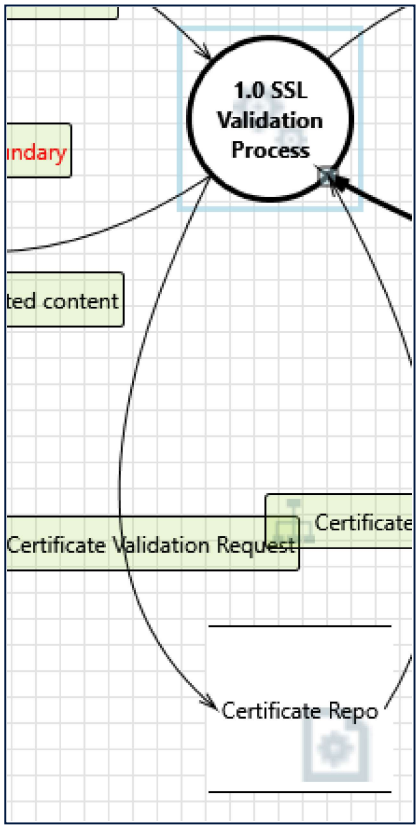


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	15
Needs Investigation	0
Mitigation Implemented	17
Total	32
Total Migrated	0

Interaction: Certificate Validation Request



1. Potential Excessive Resource Consumption for SSL Certificate Process or Certificate Repo [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: Does 1.0 SSL Validation Process or Certificate Repo take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: Yes, the if the certificates is not validated then the process will timeout which is common in all the certificate validation process.

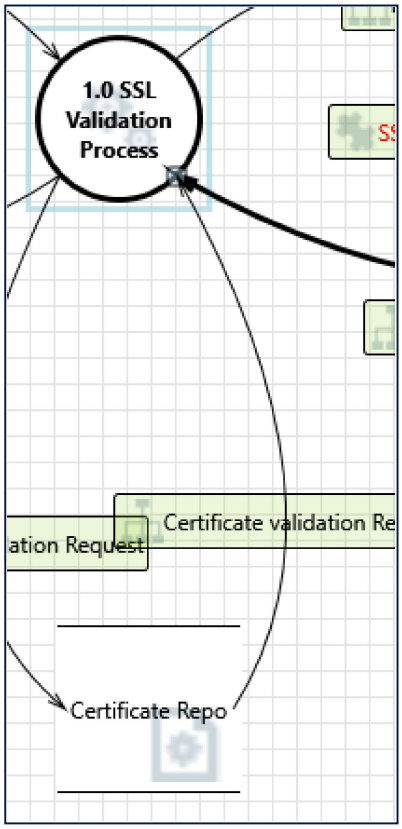
2. Spoofing of Destination Data Store Certificate Repo [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: Certificate Repo may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Certificate Repo. Consider using a standard authentication mechanism to identify the destination data store.

Justification: The certificate repo will be stored internally in the server, there is robust validation for the server login and in case of any duplication the certificates will not be validated

Interaction: Certificate validation Response



3. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Certificate Repo can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: The access to the certification will be restricted to the administrator, there will be different file system privileges placed in the server to mitigate this threat

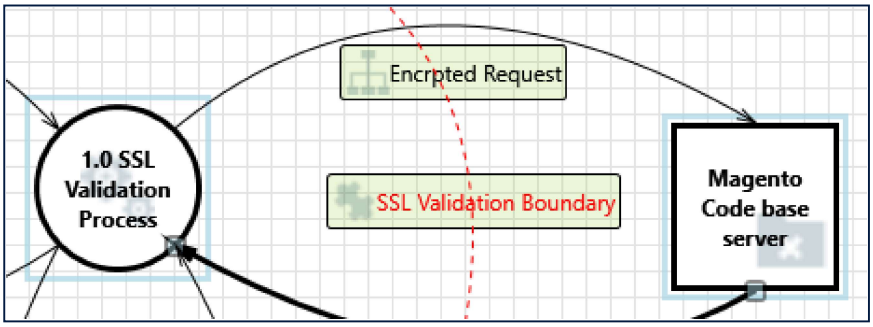
4. Spoofing of Source Data Store Certificate Repo [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Certificate Repo may be spoofed by an attacker and this may lead to incorrect data delivered to 1.0 SSL Validation Process. Consider using a standard authentication mechanism to identify the source data store.

Justification: Already addressed in other threats

Interaction: Encrpted Request



5. Data Flow Encrpted Request Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Not completely related to the magento SSL certificate process

6. External Entity Magento Code base server Potentially Denies Receiving Data [State: Not Applicable] [Priority: High]

Category: Repudiation

Description: Magento Code base server claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Already addressed in the other threats

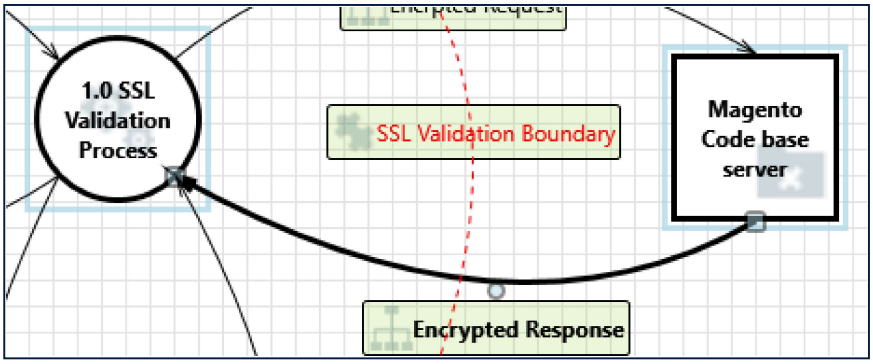
7. Spoofing of the Magento Code base server External Destination Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Magento Code base server may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Magento Code base server. Consider using a standard authentication mechanism to identify the external entity.

Justification: Once the identity is verified then the request will be processed in the Validation process, in case of the SSL stripping attacks the certificate will handle this type of requests and mitigate the spoofing

Interaction: Encrypted Response



8. Elevation Using Impersonation [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 SSL Validation Process may be able to impersonate the context of Magento Code base server in order to gain additional privilege.

Justification: Not completely related to the SSL certificate process

9. Spoofing the Magento Code base server External Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: Magento Code base server may be spoofed by an attacker and this may lead to unauthorized access to 1.0 SSL Validation Process. Consider using a standard authentication mechanism to identify the external entity.

Justification: Already addressed in other threats

10. Cross Site Request Forgery [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: already addressed in other threats

11. Elevation by Changing the Execution Flow in 1.0 SSL Validation Process [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 SSL Validation Process in order to change the flow of program execution within 1.0 SSL Validation Process to the attacker's choosing.

Justification: Already addressed in the other threats

12. SSL Certificate Process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Applicable] [Priority: High]

Category: Elevation Of Privilege

Description: Magento Code base server may be able to remotely execute code for 1.0 SSL Validation Process.

Justification: This is not in the scope of the SSL certificates process, but the admin need to keep the privileges in the Magento servers for running remote servers

13. Data Flow Encrypted Response Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: Not completely related to the SSL certificates and Validation process of Magento

14. Potential Process Crash or Stop for SSL Certificate Process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: 1.0 SSL Validation Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: To maintin the availibility the user authentication server and the code base server are differentiated in the Magento architecture

15. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across Encrypted Response may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: The complete data flow will be encrypted with the help of the SSL certificates in Magento. Magento kind of makes it mandatory to use the SSL certificate

16. Potential Data Repudiation by SSL Certificate Process [State: Not Applicable] [Priority: High]

Category: Repudiation

Description: 1.0 SSL Validation Process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Not completely related to the Magento SSL certificate and process

17. Potential Lack of Input Validation for SSL Certificate Process [State: Not Applicable] [Priority: High]

Category: Tampering

Description: Data flowing across Encrypted Response may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 SSL Validation Process or an elevation of privilege attack against 1.0 SSL Validation Process or an information disclosure by 1.0 SSL Validation Process. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: Not completely related to the SSL certificates, but there is proper data validation approaches in Magento

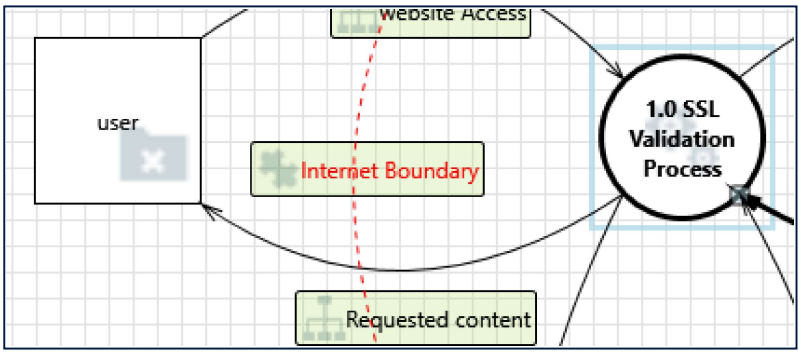
18. Spoofing the SSL Certificate Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: 1.0 SSL Validation Process may be spoofed by an attacker and this may lead to information disclosure by Magento Code base server. Consider using a standard authentication mechanism to identify the destination process.

Justification: There is a robust authentication process to validate the certificate using the CA certificate in the SSL which cannot be spoffed by the attacker

Interaction: Requested content



19. Spoofing of the user External Destination Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: user may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of user. Consider using a standard authentication mechanism to identify the external entity.

Justification: Not completely related to SSL context, but there is robust authentication mechanism placed in Magento to Validate the user

20. Data Flow Requested content Is Potentially Interrupted [State: Not Applicable] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: This case is not completely related to the Magneto SSL Validation Process

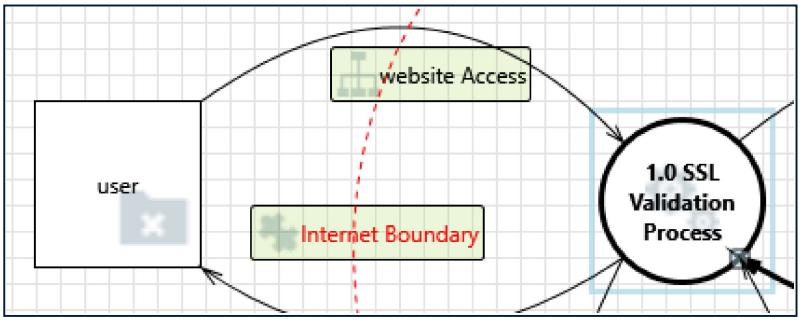
21. External Entity user Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: user claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: There will be record for the complete user data and it will be completely encrypted

Interaction: website Access



22. Spoofing the user External Entity [State: Not Applicable] [Priority: High]

Category: Spoofing

Description: user may be spoofed by an attacker and this may lead to unauthorized access to 1.0 SSL Validation Process. Consider using a standard authentication mechanism to identify the external entity.

Justification: Already addressed in other threats

23. Elevation Using Impersonation [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: 1.0 SSL Validation Process may be able to impersonate the context of user in order to gain additional privilege.

Justification: SSL Process cannot impersonate user because the unique sessions tokens will be given to the user after login. In case of any impersonation that token will not be validated and session will be closed.

24. Cross Site Request Forgery [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: Magento provides option to secure all the webpages with the help of the SSL certificate, there are even options to use the SSL certificates in specific webpages like ADMIN, Payment etc

25. Elevation by Changing the Execution Flow in SSL Certificate Process [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 SSL Validation Process in order to change the flow of program execution within 1.0 SSL Validation Process to the attacker's choosing.

Justification: WIth the help of robust SSL certificates, it will be hard for attackers to exploit flow programs of SSL Validation process

26. SSL Certificate Process May be Subject to Elevation of Privilege Using Remote Code Execution [State: Mitigation Implemented] [Priority: High]

Category: Elevation Of Privilege

Description: user may be able to remotely execute code for 1.0 SSL Validation Process.

Justification: Robust CA certificate for SSL certificates will mitigate this threat. Magento will options to configure custom certificates with robust CA certificates

27. Data Flow website Access Is Potentially Interrupted [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: WIth the help of robust SSL certificates, it will be hard for attackers to exploit flow programs of SSL Validation process

28. Potential Process Crash or Stop for SSL Certificate Process [State: Mitigation Implemented] [Priority: High]

Category: Denial Of Service

Description: 1.0 SSL Validation Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: To mitigate this SSL Validation process will be running on the Magento server where the code is not present. Which will help server to process the request fastly and user validation will happen here to stop denial attacks

29. Data Flow Sniffing [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure

Description: Data flowing across website Access may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: The complete data will be encrypted with the help of the SSL certificates in Magento

30. Potential Data Repudiation by SSL Certificate Process [State: Mitigation Implemented] [Priority: High]

Category: Repudiation

Description: 1.0 SSL Validation Process claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: Session tokens will be present for the each user session which will have a record of the source, time and summary of the input data.

31. Potential Lack of Input Validation for SSL Certificate Process [State: Mitigation Implemented] [Priority: High]

Category: Tampering

Description: Data flowing across website Access may be tampered with by an attacker. This may lead to a denial of service attack against 1.0 SSL Validation Process or an elevation of privilege attack against 1.0 SSL Validation Process or an information disclosure by 1.0 SSL Validation Process. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: The complete input data will be encrypted by the Magento with the help of the SSL certificates and it has the input validators to check the user inuts.

32. Spoofing the SSL Certificate Process Process [State: Mitigation Implemented] [Priority: High]

Category: Spoofing

Description: 1.0 SSL Validation Process may be spoofed by an attacker and this may lead to information disclosure by user. Consider using a standard authentication mechanism to identify the destination process.

Justification: Valid authentication mechanism is presnt in Magento it is even secured with Multi factor authentication