Partner Guide: Ensuring Security and Integrity in Certificate Operations

Introduction

As a Certificate Authority (CA) and provider of trust services, we are committed to maintaining the highest standards of security and trust in the digital certificates we issue and in our identity validation processes.

This guide is specifically designed for our partners. Partners play a crucial role in collecting validation evidence, submitting it to us, and facilitating the issuance of certificates through their partner-branded subroots (subCA).

The purpose of this guide is to ensure the integrity and security of the validation evidence submission process and certificate lifecycle management.

Our partners interact with certificate lifecycle processes via a designated API or through an account within the CertManager portal.

Secure Collection of Validation Evidence for Various Validation Types

1. Data Minimization

- Collect only the essential validation evidence required for certificate issuance. Avoid collecting unnecessary or sensitive information to ensure compliance with data protection standards.

2. Secure Collection Methods

- Use encrypted channels (such as HTTPS, password-protected and encrypted customer accounts, encrypted forms, encrypted e-mails and password-protected attachments) for gathering validation evidence from end-users to ensure that sensitive data is protected.
- Sign all email correspondence sent to your clients with an S/MIME certificate to ensure its integrity.

3. Access Control

- Restrict access to the validation evidence for authorized personnel only. Enforce multi-factor authentication (MFA) to strengthen security and reduce risks of unauthorized access.

4. Data Integrity

- Implement measures to ensure that validation evidence is not altered during collection. This includes both technical measures and process oversight.

5. Subscriber Validation

- When validating the subscriber data, it is essential to ensure that our standards are strictly adhered to. Partners must not accept any verifications that raise suspicions or do not meet Certum requirements. Additionally, any instances of suspected fraud in the verification process, even if discovered after the certificate issuance, should be reported to us immediately.

Safe Submission of Validation Evidence to Certum

1. API Security

- Use the designated API or CertManager portal for submitting validation evidence. Validation material delivery is also possible via e-mail, please ensure that if you’re using this method – you're sending encrypted e-mails and/or password-protected attachments.

2. Upload via API/CertManager

- When uploading evidence directly through the CertManager portal, ensure that it is associated strictly with the relevant certificate order. Do not upload evidence unrelated to the order in question.

3. Regular Audits

- Conduct regular audits of your submission logs to detect and prevent any unauthorized submissions or inconsistencies in the process.

4. Incident Response

- Have a clear incident response plan in place for any discrepancies or breaches in the submission process. In case of any irregularities, notify us immediately for investigation and resolution.

Best Practices for Using the Certificate Lifecycle Operations API

1. Rate Limiting

- Be aware of the rate limits imposed on the API to avoid unintentional service disruptions and ensure smooth operation of your processes.

2. Monitoring and Logging

- Implement continuous monitoring of API activity. Maintain comprehensive logs of all interactions and review them regularly for any signs of suspicious or unauthorized activity.
- Regularly collect and periodically verify which of your employees have login credentials to CertManager. Revoke access in the event of an employee's removal or role change.
- Authenticate only the IP addresses of machines over which you have full control and that meet high system security standards for API connections. Periodically monitor the list of authenticated IP addresses and report the removal of those that should no longer have API access.

3. Error Handling

- Develop clear procedures for handling API errors. Address any discrepancies or issues promptly and notify us for assistance when necessary.

Maintaining a Secure Website and Server Infrastructure

1. Proper TLS Server Configuration

- Ensure that your server is configured to use only strong cryptographic ciphers and protocols. Regularly update and patch servers to eliminate vulnerabilities.

2. Operating System Hardening

- Minimize the number of services running on your servers. Apply security patches in a timely manner and utilize configuration management tools to strengthen security posture.
- Monitor and manage user roles to ensure that each individual has the minimum required permissions, following the principle of least privilege.

3. Vulnerability Management

- Regularly scan your website and servers for common vulnerabilities, including but not limited to SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF), and promptly address any issues.

4. Password Strength

- Ensure that passwords are strong and difficult to guess. Encourage the use of multi-factor authentication (MFA) for added protection, especially for critical systems

---

CA/B Forum Network and Certificate Systems Security Requirements

1. Quarterly Vulnerability Scans

- Perform vulnerability scans every quarter to identify and mitigate any security risks. Act promptly on identified weaknesses.

2. Annual Penetration Testing

- Engage in penetration testing at least once per year. Use these tests to uncover potential weaknesses in your infrastructure and certificate management practices.

3. Adherence to Security Standards

- Ensure compliance with the CA/B Forum Network and Certificate Systems Security Requirements. This is vital for maintaining the trust and integrity of the certificate issuance and lifecycle process.

Promoting End-User Best Practices for Key Management

1. Educating on Key Generation

- Instruct end-users to use system/server certificate manager tools for key generation and CSR creation to ensure compatibility with industry standards and enhanced security.

2. Key Length and Algorithm

- Recommend end-users to use strong cryptographic algorithms and key lengths, even higher than RSA 2048-bit to secure their certificates.

3. Secure Storage of Private Keys

- Advise end-users to store their private keys securely, preferably in hardware security modules (HSMs) or encrypted storage solutions.

4. Key Rotation and Revocation

- Encourage users to rotate their keys regularly and to revoke any keys that are no longer needed or have been compromised. Implement a policy for prompt key revocation in case of security incidents.

5. Disaster Response Strategy

- Develop a robust disaster response plan for handling key compromise, loss, or corruption. This should include clear steps for recovering keys or mitigating any associated risks.

Ensuring End-User Communication for Certificate Status and Validation Codes

In scenarios where partners don't want Certum to send information and/or verification e-mails directly to end-users, partners are responsible for ensuring these communications are delivered through alternative, secure channels. Failure to provide timely and accurate validation information may delay certificate issuance or compromise user experience. Partners must implement reliable mechanisms to:

- Notify end-users about the status of their certificate request.
- Provide required domain verification links.
- Ensure delivery methods are secure, trackable, and comply with data protection requirements.

Conclusion

Trust in our Certificate Authority and our partners is essential for maintaining the integrity of the digital certificate ecosystem. By following these best practices, you help protect the certificate issuance process, safeguard end-user data, and uphold the trust in the services we provide.

We strongly encourage our partners to strictly adhere to the outlined principles, which support the security and integrity of certificate-related operations and ensure alignment with industry's best practices. Should you have any questions or require

further information, please do not hesitate to contact us. Together, we can preserve reliability and trust in our digital services.