Main 1.16. KSK Rotation: Describe the processes and procedures used to practice and ensure successful KSK rotation in both emergency and non-emergency situations, including coordination with DNSSEC RSP and IANA.

(I) KSK Rotation Process in Non-emergency Situations

1. **Pre-planning and Preparation**

- **Formulate rotation plan**: Domain administrators formulate detailed KSK rotation plans in advance, clarifying key parameters such as rotation timelines, encryption algorithms used, key lengths, etc. For example, use RSA SHA256 algorithm (2048-bit KSK + 1024-bit ZSK) to implement zone data signing, and set KSK to rotate every 36 months. The plan should cover timelines for all stages including key generation, distribution, and signature update.
- **Evaluate system compatibility**: Evaluate the compatibility of existing DNS servers, resolvers, and related software to ensure they can support new KSK and operations during rotation. For example, check if DNS server software versions support new encryption algorithms, and upgrade them in advance if not.
- **Notify relevant parties**: Send advance notifications to Internet service providers, enterprise network administrators, other DNS resolution system operators, DNS resolution system software developers, system integrators, and hardware/software distributors installing or sending root zone "trust anchors," informing them of the upcoming KSK rotation plan to facilitate their preparation, such as software updates and configuration adjustments.

2. **New KSK Generation**

- **Key generation environment preparation**: Use secure key generation tools and environments to ensure the security of the key generation process. For example, generate KSK using hardware encryption modules (HSMs), which provide physical security protection to prevent key theft during generation.
- **Generate key pairs**: Generate new KSK public and private key pairs according to predetermined encryption algorithms and key length requirements. The generated private keys should be properly safeguarded with multiple encryption and access control measures to ensure only authorized personnel can access them.

3. **Coordination with DNSSEC RSP**

- **Submit new key information**: Submit the newly generated KSK public key information to the DNSSEC RSP, which is responsible for maintaining DNSSEC-related policies and data. Submit information through secure communication channels (e.g., encrypted email, dedicated secure data transmission interfaces) to ensure information transmission security and integrity.
- **Verification and review**: The DNSSEC RSP verifies and reviews the submitted new KSK public key information, checking whether the key format is correct and meets relevant security standards. After review, the DNSSEC RSP incorporates the new key information into its management system and updates records accordingly.

4. **Coordination with IANA**

- **Notify IANA**: Send an official notification to IANA informing it of the upcoming KSK rotation operation. The notification includes rotation time, new KSK-related information (e.g., public key fingerprint), etc., to enable IANA to coordinate and record in global DNS root zone management.
- **Follow IANA processes**: Complete procedures and operations related to KSK rotation in accordance with IANA-specified processes and requirements. For example, submit necessary documents and information within specific time windows and cooperate with IANA for related testing and verification.

5. **Zone Signature Update**

- **Sign with new KSK**: After new KSK generation and coordination with DNSSEC RSP and IANA, use the new KSK to encrypt and sign zone signature keys (ZSKs). This step is a key link in establishing a new trust chain to ensure subsequent DNS resolution processes can verify data authenticity.
- **Update DNSKEY resource records**: Publish DNSKEY resource records containing the new KSK public key to authoritative DNS servers, enabling other DNS servers and resolvers to obtain new key information. Meanwhile, ensure DNSKEY resource record validity periods are set reasonably to balance key security and avoid additional overhead from frequent updates.

6. **Key Distribution and Propagation**

- **Distribute to resolvers**: Distribute new KSK public keys to Internet service providers, enterprise network administrators, and other relevant parties operating verification resolution systems through secure means. Distribution can be done via pre-configured secure channels (e.g., HTTPS download, dedicated key distribution servers) to ensure resolvers can timely obtain new key information for verification during DNS resolution.
- **Propagation and cache update**: As new DNSKEY resource records and related signature information propagate in the DNS system, each DNS server and resolver will gradually update key information in their caches. During this process, closely monitor propagation to ensure new key information propagates to the entire DNS system within a reasonable time, avoiding resolution failures due to delayed cache updates.

7. **Monitoring and Verification**

- **Monitor resolution status**: Continuously monitor DNS resolution status during and after KSK rotation, checking for resolution failures, increased latency, or other issues caused by key updates. Real-time track and analyze resolution processes of key domains by deploying specialized monitoring tools.
- **Verify signature validity**: Use DNSSEC verification tools to verify signatures in DNS responses, ensuring the new KSK can correctly verify zone data signatures and safeguard DNS data authenticity and integrity. Conduct verification tests regularly to promptly identify and resolve potential signature verification issues.

(II) KSK Rotation Procedures in Emergency Situations

1. **Emergency Response Activation**

- **Security incident detection and reporting**: When emergency situations potentially affecting KSK security (such as key leaks or severe security attacks) are detected, relevant security monitoring systems should

immediately issue alerts and report detailed incident information to domain administrators, including incident occurrence time, possible impact scope, suspected security vulnerabilities, etc.

- **Evaluate incident impact**: Domain administrators promptly organize security experts to evaluate the incident's impact on KSK security and possible consequences. For example, analyze key leakage channels and scope, and assess the possibility of hackers using leaked keys to forge DNS data.
- **Initiate emergency response procedures**: Based on incident impact assessment results, once it is determined that KSK rotation is needed to address the emergency, immediately initiate pre-formulated emergency response procedures. The procedures should clearly specify the responsibilities and tasks of each department and personnel during emergency response to ensure efficient emergency response.

2. **Rapid Key Generation and Preparation**

- **Emergency key generation**: In emergency situations, use pre-prepared secure key generation environments and tools to rapidly generate new KSK public and private key pairs. Compared to non-emergency situations, this process requires stricter security control and time management to ensure usable keys are generated in the shortest time.
- **Simplify preparation processes**: Simplify some non-critical pre-preparation work to prioritize key generation and subsequent rotation operations. For example, appropriately reduce comprehensive system compatibility testing while ensuring security, only conducting rapid verification of key components.

3. **Emergency Coordination with DNSSEC RSP**

- **Activate emergency communication channels**: Use pre-established emergency communication channels (such as dedicated emergency communication lines, emergency contact groups) to immediately contact the DNSSEC RSP, explaining the severity and urgency of the emergency and the upcoming emergency KSK rotation operation.
- **Expedite review and support**: Request the DNSSEC RSP to urgently review and process newly submitted KSK public key information. The DNSSEC RSP should activate emergency response mechanisms, allocate sufficient resources, complete verification and review of new keys in the shortest time, and provide necessary technical support and guidance to ensure emergency KSK rotation proceeds smoothly.

4. **Emergency Coordination with IANA**

- **Emergency notification and communication**: Send emergency notifications to IANA via the fastest and most reliable means, detailing the emergency and emergency KSK rotation plan. Maintain close communication with IANA, promptly responding to IANA's inquiries and requirements, and cooperating with IANA in global DNS root zone-related emergency coordination.
- **Apply for special processes**: Depending on the particularity of the emergency, apply to IANA for activating special emergency processes when necessary to expedite procedures and operations related to KSK rotation, ensuring global DNS root zone key information can be rapidly adjusted in emergencies to safeguard DNS system security and stability.

5. **Emergency Zone Signature Update and Propagation**

- **Prioritize updating critical zones**: In emergency situations, prioritize signature updates for critical domain zones, use newly generated KSK to encrypt and sign ZSKs, and promptly publish updated signature information to authoritative DNS servers. Simultaneously, update signatures for other important zones in priority order to ensure the core part of the DNS system can rapidly restore security status.
- **Accelerate propagation mechanisms**: Adopt acceleration propagation mechanisms, such as increasing synchronization frequency between DNS servers and optimizing cache update strategies, to enable new signature information and key information to rapidly propagate in the DNS system, reducing security risks caused by information propagation delays. Specialized DNS data propagation acceleration tools or technologies can be used to improve propagation efficiency.

6. **Emergency Monitoring and Recovery**

- **Strengthen monitoring efforts**: During and after emergency KSK rotation, increase monitoring intensity of the DNS system, real-time monitoring DNS resolution performance, signature verification status, and presence of abnormal traffic, etc. Deploy more monitoring nodes and tools to comprehensively and multi-dimensionally monitor the DNS system, promptly discovering and handling potential issues.
- **Recovery and summary**: When the DNS system returns to normal operation, summarize and evaluate the entire emergency response process, analyze problems and deficiencies in emergency response, summarize experience, and optimize and improve emergency response procedures and related plans to enhance capabilities for addressing similar emergencies in the future.