# 🎯 PV25 요구사항 정의

프로젝트에 대한 최상위 명세 문서입니다.

## 고객 요구사항 명세 (CRS)

### 핵심 기능

| ID | 요구사항 상세 설명 | 분류 | 중요도 | 대응 SRS | 비고 |
|---|---|---|---|---|---|
| PV25-CRS-CORE-01 | 인증서를 발급할 수 있어야 한다(특히 다음 용도의 인증서를 발급할 수 있어야 한다):<br>• TLS / 제어기 내 전자서명 / 제어기 내 암호화 /<br>• SGW Secure Unlock(0x29) / SGW Secure Access (0x29 or 0x27)<br>• (인증서 유형 일람[1]참조) | 인증서 생명주기 | HIGH | ↗ PV25-FR-02 | |
| PV25-CRS-CORE-02 | 인증서의 폐지가 가능해야 한다. | 인증서 생명주기 | HIGH | ↗ PV25-FR-03 | |
| PV25-CRS-CORE-03 | 인증서 체인 구성을 지원해야 한다. | 인증서 생명주기 | HIGH | ↗ PV25-FR-01 | |
| PV25-CRS-CORE-04 | 기타 인증서의 발급, 재발급, 갱신, 폐기, 조회 관련 필수 기능이 모두 존재해야 한다. | 인증서 생명주기 | HIGH | ↗ PV25-FR-04<br>↗ PV25-FR-05 | |

| | | | | | |
|---|---|---|---|---|---|
| PV25-CRS-CORE-05 | 인증서 폐지 상태를 실시간(OCSP) 및 주기적(CRL)으로 검증할 수 있어야 한다.<br>• CRL을 지원해야 한다<br>• OCSP를 지원해야 한다(OCSP Responder 확장 형태로)<br>• (옵션)RTCS, SCVP, TSP를 지원해야 한다 | 폐지 상태 검증 | HIGH | ↗ PV25-FR-10<br>↗ PV25-FR-11 | |
| PV25-CRS-CORE-06 | OCSP Stapling을 지원해야 한다. | 폐지 상태 검증 | LOW | | |
| PV25-CRS-CORE-07 | 활성화된 제어기로부터 발생할 수 있는 OCSP 트래픽을 감당할 수 있어야 한다. | 폐지 상태 검증 | HIGH | ↗ PV25-FR-24<br>↗ PV25-NFR-02 | |
| PV25-CRS-CORE-08 | 인증서 관리를 위해 산업 표준 프로토콜(CMP)을 지원해야 한다.<br>• CMP를 지원해야 한다(CMP는 CA만이 노출한다. RRA는 노출된 API를 권한관리를 적용하여 다시 노출할 수 있다)<br>• (옵션)PKCS#10을 지원해야 한다<br>◦ PKCS#10을 지원할 경우, SCEP의 형태로 지원한다 | 프로토콜 지원 | HIGH | ↗ PV25-FR-02<br>↗ PV25-FR-03<br>↗ PV25-FR-04<br>↗ PV25-FR-05 | |
| PV25-CRS-CORE-09 | 지원 표준 일람[3]을 관리하여야 한다. | 표준 지원 | MED... | | |
| PV25-CRS-CORE-10 | 다양한 용도(TLS, 코드 서명 등)에 맞는 인증서 프로파일(정책)을 생성하고 관리할 수 있어야 한다. | 인증서 프로파일 | HIGH | ↗ PV25-FR-13 | Ceer PKI 요구사항 |

| | | | | | |
|---|---|---|---|---|---|
| PV25-CRS-CORE-11 | 인증서 프로파일은 유효기간으로 초/분/시간/일/월/연 등의 단위 주기 및, overlap 기간을 복합적으로 허용하여야 한다. | 인증서 프로파일 | MED... | | Sep 2, 2025 대표님 요구사항 |
| PV25-CRS-CORE-12 | 알고리즘 지원 일람[2]내 알고리즘을 지원해야 한다.<br>• TLS 1.3이 요구하는 알고리즘은 필수로 지원해야 한다<br>• (옵션)그 외 알고리즘 | 알고리즘 지원 | HIGH | ↗ PV25-FR-25 | Ceer PKI 요구사항 |
| PV25-CRS-CORE-13 | 인증서의 Serial Number는 RFC 5280의 권고사항대로 최대 20 bytes 랜덤값을 가질 수 있어야 한다. | 기타 | HIGH | | |
| PV25-CRS-CORE-14 | 라이센스적용이 가능하여야 한다. | 기타 | MED... | | |

**관리 및 운영**

| ID | 요구사항 상세 설명 | 분류 | 중요도 | 대응 SRS | 비고 |
|---|---|---|---|---|---|
| PV25-CRS-MGMT-01 | 간이 LRA인 Reference RA를 구현해야 한다. | 관리 페이지 | HIGH | ↗ PV25-FR-06<br>↗ PV25-FR-07<br>↗ PV25-FR-08<br>↗ PV25-FR-09<br>↗ PV25-FR-12 | 과제 조직이 RA를 개발할 때 시작점으로 사용할 수 있는 Reference 제공이 목적임. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | ↗ PV25-FR-14<br>↗ PV25-FR-15<br>↗ PV25-FR-16<br>↗ PV25-FR-17<br>↗ PV25-FR-18<br>↗ PV25-FR-19<br>↗ PV25-FR-20<br>↗ PV25-FR-21 | |
| PV25-CRS-MGMT-02 | 제품 버전을 표시하여야 한다. | 관리 페이지 | HIGH | ↗ PV25-FR-26 | |
| PV25-CRS-MGMT-03 | 다음 시스템 관리 기능을 제공하여야 한다:<br>• 계정 목록 조회 / 계정 상세 조회 / 계정 추가, 수정, 삭제<br>• 로그인(옵션: MFA) / 로그인 이력 / 세션 지원 | 관리 페이지 | HIGH | ↗ PV25-FR-23 | |
| PV25-CRS-MGMT-04 | 시스템 최초 설치 시, 시나리오(기존 복원/신규 생성/하위 참여)에 따른 명확한 가이드를 제공해야 한다. | 초기 설정 | HIGH | ↗ PV25-NFR-12 | |

| | | | | | |
|---|---|---|---|---|---|
| PV25-CRS-MGMT-05 | Root CA 및 여러 단계의 중간(Intermediate) CA로 구성된 인증서 체인을 구성하고 관리할 수 있어야 한다. | CA 체인 관리 | HIGH | ↗ PV25-FR-01 | |
| PV25-CRS-MGMT-06 | 인증서 만료, CA 갱신 등 주기적인 작업을 자동으로 처리하고 알림을 발생시키는 스케줄링 기능이 있어야 한다. | 스케줄러 | HIGH | ↗ PV25-FR-27 | |
| PV25-CRS-MGMT-07 | 인증서 발급현황 통계가 '일, 주, 월' 등 단위로 제공되어야 한다. | 통계 | HIGH | ↗ PV25-FR-23 | Ceer PKI 요구사항 |
| PV25-CRS-MGMT-08 | CSR 요청기록 통계가 '일, 주, 월' 등 단위로 제공되어야 한다. | 통계 | HIGH | ↗ PV25-FR-23 | Ceer PKI 요구사항 |
| PV25-CRS-MGMT-09 | 인증서 발급 현황, 서버 상태 등 시스템의 핵심 지표를 한눈에 파악할 수 있는 대시보드를 제공해야 한다. | 관리 페이지 | MED... | | |
| PV25-CRS-MGMT-10 | 서버 부하율(CPU, Memory)이 표시되어야 한다. | 관리 페이지 | MED... | | |
| PV25-CRS-MGMT-11 | 인증서 만료 임박, 시스템 오류 등 주요 이벤트 발생 시 관리자가 즉시 인지할 수 있도록 Slack, Teams 등 외부 채널로 알림을 보내야 한다. | 알림 | LOW | | 내부망 환경을 위해 로그인 시 이슈를 알려주는 기능도 포함한다. 작업량을 고려하여 로그인 시 이슈를 알려주는 기능부터 개발할 수 있다. |

**정책 및 워크플로우**

| ID | 요구사항 상세 설명 | 분류 | 중요도 | 대응 SRS | 비고 |
|---|---|---|---|---|---|
| PV25-CRS-POLICY-01 | 인증서 정책 설정 시, 특정 필드(예: OU, SAN)에 허용되는 값의 규칙(정규식 등)을 정의하고 강제할 수 있어야 한다.<br>• CA/B 프로파일 등의 강제가 가능한 수준으로 제약이 고도화되어야 한다 | 필드 값 제약 | HIGH | ↗ PV25-FR-13 | 기간에 맞추기 어려울 경우, CA/B 프로파일 수준의 Validation은 zlint등 3rd party 활용 가능. |
| PV25-CRS-POLICY-02 | 공통 정책을 '템플릿'으로 만들어두고, 다른 정책들이 이를 상속받아 일부만 수정하여 사용할 수 있어야 한다. | 템플릿 상속 | MED... | ↗ PV25-FR-13 | |
| PV25-CRS-POLICY-03 | 중요 인증서 발급 요청 시, 자동 발급 대신 지정된 승인권자의 승인을 거치도록 하는 워크플로우 기능이 있어야 한다. | 승인 워크플로우 | MED... | | 제품 완성도 기준으로는 우선순위가 높은 기능이나, 일정 제약으로 인해 우선순위를 낮춤. |

**보안 및 인프라**

| ID | 요구사항 상세 설명 | 분류 | 중요도 | 대응 SRS | 비고 |
|---|---|---|---|---|---|
| PV25-CRS-SEC-01 | CA의 개인키는 HSM과 같은 보안 하드웨어에 안전하게 저장 및 연동할 수 있어야 한다.<br>• HW가 없어도 기동할 수 있는 옵션 또한 존재해야 한다 | 키 관리 | HIGH | ↗ PV25-FR-22<br>↗ PV25-NFR-05 | HSM은 FIPS 140-2 Level 3 규격을 준수하는 것을 사용해야 한다. |
| PV25-CRS-SEC-02 | P11을 통해 카드형 HSM, 네트워크 HSM, KMS 등과 연동 가능해야 한다. | 키 관리 | HIGH | | |
| PV25-CRS-SEC-03 | TLS 1.3 등 최신 보안 표준에서 요구하는 암호화 알고리즘을 지원해야 한다. | 알고리즘 | HIGH | | |

| | | | | | |
|---|---|---|---|---|---|
| PV25-CRS-SEC-04 | 시스템 장애 시 서비스를 신속하게 복구할 수 있는 재해 복구(DR) 방안을 지원해야 한다. | 재해 복구 (DR) | HIGH | ↗ PV25-FR-22 | 최저한도로 2~3대 장비로 DR 구성은 해야 함. |

**고급/확장 기능**

| ID | 요구사항 상세 설명 | 분류 | 중요도 | 대응 SRS | 비고 |
|---|---|---|---|---|---|
| PV25-CRS-ADV-01 | (선택사항) 데이터 암호화 용도의 인증서에 한해, 개인키 분실 시 관리자가 안전한 절차를 통해 복구할 수 있는 기능을 제공해야 한다. | 키 복구 (선택) | LOW | | 키 복구는 다중 관리자 승인(M of N)을 거쳐야만 수행되도록 엄격한 통제 절차를 구현한다. |
| PV25-CRS-ADV-02 | (로드맵) 서버 인증서 발급 자동화를 위해 표준 프로토콜인 ACME를 지원해야 한다. | ACME 지원 | LOW | | |
| PV25-CRS-ADV-03 | (선택사항) LDAP를 지원하여야 한다. | LDAP 지원 | LOW | | |

---

## 🔖 SRS 정제

⚠️ **2025년 Iteration 1(** Jul 1, 2025 ~ Sep 30, 2025 **) 기간 개발 대상은 아래 SRS 내용의 하위 집합으로 합니다.**

**기능 요구사항 (FR)**

| ID | 요구사항 상세 설명 | 중요도 | 비고 |
|---|---|---|---|
| PV25-FR-01 | Software Appliance 형태로, Root/Intermediate등 CA 체인 깊이 N 생성을 지원한다 | HIGH | 단일 CA만으로도 지원할 수 있도록 구현한다. |

| | | | |
|---|---|---|---|
| | | | 단, 필요시 CA를 복합으로 구성할 수 있다. |
| PV25-FR-02 | CMP를 통한 인증서 발급 기능을 지원한다 | HIGH | CMP 기능은 CA가 제공하고, R.RA는 중계한다. |
| PV25-FR-03 | CMP를 통한 인증서 폐지 기능을 지원한다 | HIGH | CMP 기능은 CA가 제공하고, R.RA는 중계한다. |
| PV25-FR-04 | CMP를 통한 인증서 재발급 기능을 지원한다 | HIGH | CMP 기능은 CA가 제공하고, R.RA는 중계한다. |
| PV25-FR-05 | CMP를 통한 인증서 갱신 기능을 지원한다 | HIGH | CMP 기능은 CA가 제공하고, R.RA는 중계한다. |
| PV25-FR-06 | 인증서 발급 기능을 지원한다 | HIGH | R.RA 사용자의 편의성을 위해, R.RA가 CMP 기능을 wrapping한다. |
| PV25-FR-07 | 인증서 폐지 기능을 지원한다<br>• HOLD 편의기능은 제공하지 않는다 | HIGH | R.RA 사용자의 편의성을 위해, R.RA가 CMP 기능을 wrapping한다. |
| PV25-FR-08 | 인증서 재발급 기능을 지원한다 | HIGH | R.RA 사용자의 편의성을 위해, R.RA가 CMP 기능을 wrapping한다. |
| PV25-FR-09 | 인증서 갱신 기능을 지원한다 | HIGH | R.RA 사용자의 편의성을 위해, R.RA가 CMP 기능을 wrapping한다. |
| PV25-FR-10 | CRL을 통한 인증서 폐지를 지원한다<br>• CRL 자동 발행 (≤10 min 등 주기 설정 가능) | HIGH | CRL 수동 발행이 필요없도록, 자동화 구성을 지원한다. |
| PV25-FR-11 | OCSP를 통한 인증서 폐지를 지원한다<br>• VA Pod에서 OCSP 응답. OCSP가 필요하지 않은 경우 VA off 가능(Helm 값 `va.enabled=false` 등) | HIGH | VA는 OCSP Responder로 기능을 한정한다. |
| PV25-FR-12 | 기 발행된 인증서의 조회 및 다운로드를 지원한다 | HIGH | 관리기능 |

| | | | |
|---|---|---|---|
| PV25-FR-13 | 인증서 발급 관리를 위한 정책 추가 기능을 지원한다<br>• 정책은 단순 필드값 입력만이 아닌, 필드 유효성 검사도 지원해야 한다<br>• X.509 v3 전체 필드에 대한 정책 설정이 가능해야 한다<br>• 세부 예:<br>◦ CABF BR 기본 프로필 + 사용자 정의(CCCDK, ISO 15118-2 등) 정책 관리 기능 | HIGH | 관리기능<br>• 인증서 프로필은 yaml/json 등의 형태를 지원해야 한다(복잡한 설정을 지원할 수 있게 하기 위함)<br>• yaml/json 등의 형태의 프로필을 import 해올 수 있는 기능을 관리페이지에서 지원해야 한다 |
| PV25-FR-14 | 인증서 발급 정책 조회 기능을 지원한다 | HIGH | 관리기능 |
| PV25-FR-15 | CA 인증서(루트 포함) 발급 기능을 제공한다 | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |
| PV25-FR-16 | CA 인증서(루트 포함) 폐기 기능을 제공한다<br>• HOLD 편의기능은 제공하지 않는다 | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |
| PV25-FR-17 | CA 인증서(루트 포함) 재발급 기능을 제공한다 | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |
| PV25-FR-18 | CA 인증서(루트 포함) 갱신 기능을 제공한다<br>• CA 인증서 자동 갱신 (주기 설정 가능) | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |
| PV25-FR-19 | CA 인증서(루트 포함) 조회 및 다운로드 기능을 제공한다 | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |
| PV25-FR-20 | CA 인증서(루트 포함) pfx import 기능을 제공한다 | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |
| PV25-FR-21 | OCSP Signer 생성 | HIGH | • UI를 통해 지원한다<br>• 필요시 REST를 통한 기능 지원을 추가한다 |

| | | | |
|---|---|---|---|
| PV25-FR-22 | P11 Adapter 모듈이 HSM Failover(Luna↔CloudHSM) 등 HSM DR 지원 | HIGH | • ASN.1 Codec으로는 BouncyCastle을 활용한다<br>• 암호화 기능 추상화로 JCA를 사용할지, 수기 P11 추상화를 진행할지는 추가 검토한다 |
| PV25-FR-23 | Admin Web (UI) - 인증서/체인/폐지/정책/HSM 모니터링/감사 로그<br>• 와이어프레임에 상세 내역 기재 | HIGH | ⚒PV25 개발 상세 설계 및 구현 - UI기획 참조 |
| PV25-FR-24 | VA(OCSP Responder)는 Scale out 가능해야 한다 | HIGH | ↗ PV25-NFR-02 참조 |
| PV25-FR-25 | TLS 1.3이 허용하는 모든 알고리즘을 지원해야 한다 | HIGH | 이전 버전에 대한 지원은 필요해질 때마다 추가한다.<br>↗ PV25-NFR-05 참조 |
| PV25-FR-26 | 제품 버전을 표시하여야 한다 | HIGH | |
| PV25-FR-27 | 스케줄러에 의해 CA인증서가 만료되기 전 자동으로 갱신할 수 있는 설정 기능이 존재하여야 한다. | HIGH | 스케줄러 모듈은:<br>• CA 인증서 자동 갱신 로직을 트리거하고,<br>• 설정된 주기에 따라 만료 예정 인증서를 스캔하여 알림 시스템에 이벤트를 전달하는 역할을 수행한다 |

**비기능 요구사항 (NFR)**

| ID | 요구사항 | 중요도 | 비고 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| PV25-NFR-01 | 인증서 발급 성능: p95 latency ≤ 40 ms at 300 TPS, CPU ≤ 60 %<br>• 근거: 대한민국 전체 자동차 2500만대, 차량당 인증서 탑재 제어기 10개, 자동차 라이프사이클 15년 기준으로, 10 * 25,000,000 / 15 / 365 / 24 / 60 / 60 = **0.53 인증서 발행/초** 달성시 생산 대응 가능 | HIGH | 300 TPS 등 수치는 H/W 성능에 의해 제한을 받는다. 단, 저비용으로 성능을 끌어올리기 위해 KEK를 사용하는 모드를 두는 것을 고려할 수 있다. |
| PV25-NFR-02 | OCSP 검증 성능: p95 latency ≤ 40 ms at 1000 TPS, CPU ≤ 60 %<br>• 근거: 대한민국 전체 자동차 2500만대(수렴시), 일간 차량당 OCSP 요청 10회 미만 기준으로,<br>10 * 25,000,000 / 24 / 60 / 60 = **2893 OCSP/초** 지원 필요 | | |
| PV25-NFR-03 | SaaS 99.9 %, 2-node Appliance 99.9 % | HIGH | |
| PV25-NFR-04 | DB RPO ≤ 5 s, RTO ≤ 30 min | MEDIUM | |
| PV25-NFR-05 | FIPS 140-2 Lv 3 HSM, CA 키 외부 반출 금지 | HIGH | 동일 구성 복원을 위해서는 평문 키 추출이 필요할 수 있다(예: pfx import 기능 지원) |
| PV25-NFR-06 | TLS 1.3 + ECDHE PFS, SSL Labs A 등급 | HIGH | |
| PV25-NFR-07 | CABF-BR §5: 운영·물리 통제 로그 ≥ 7 년 보관 | MEDIUM | |
| PV25-NFR-08 | Observability 구성(Actuator, P8S, Grafana, etc.) | HIGH | |
| PV25-NFR-09 | 롤백 필요시 ≤ 30 min | MEDIUM | |
| PV25-NFR-10 | ARM64 & x86-64 JDK 21 이미지, K8S 1.29+ | LOW | |
| PV25-NFR-11 | Admin UI 국제화(국/영) 지원 | HIGH | |

| | | | |
|---|---|---|---|
| PV25-NFR-12 | 운영/엔지니어링용 문서: OpenAPI 3.1, 운영 가이드북, 구축/배포 설명서 | LOW | |
| PV25-NFR-13 | GitOps 배포: PR → main merge → Jenkins build & ECR push → Argo CD sync | MEDIUM | |
| PV25-NFR-14 | SaaS(EKS) / 1-node / 2-node Appliance별 설정/배포 자동화 | MEDIUM | |
| PV25-NFR-15 | CA Pod ↔ VA Pod REST 호출은 동일 네임스페이스 또는 ServiceMesh 통신 | LOW | |

---

[1] 인증서 유형 일람:

- Standard X.509 certificates
- AuthentiCode code signing certificates
- Certificates conformant to the IETF PKIX profile
- IPsec server, client, end-user, and tunneling certificates
- Qualified certificates
- Resource PKI (RPKI) certificates
- SigG certificate extensions
- S/MIME email certificates
- SSL/TLS server and client certificates
- Timestamping certificates

[2] 알고리즘 지원 일람:

| 알고리즘 | 키 크기 | 블록 크기 |
|---|---|---|
| AES | 128/192/256 | 128 |
| ~~CAST-128~~ | ~~128~~ | ~~64~~ |
| ~~DES~~ | ~~56~~ | ~~64~~ |
| ~~Triple DES~~ | ~~112 / 168~~ | ~~64~~ |
| ~~IDEA~~ | ~~128~~ | ~~64~~ |
| ~~RC4~~ | ~~2048~~ | ~~8~~ |

| ~~SHA-1~~ | ~~—~~ | ~~160~~ |
|---|---|---|
| SHA-2 / SHA-256 | — | 256 |
| ~~HMAC-SHA1~~ | ~~160~~ | ~~160~~ |
| HMAC-SHA2 | 256 | 256 |
| Diffie-Hellman | 4096 | — |
| ~~DSA~~ | ~~4096~~ | ~~—~~ |
| ECDSA | 521 | — |
| ECDH | 521 | — |
| Elgamal | 4096 | — |
| RSA | 4096 | — |

[3] 지원 표준 일람 (예시):

**ANSI X3.92, ANSI X3.106, ANSI X9.9, ANSI X9.17, ANSI X9.30-1, ANSI X9.30-2, ANSI X9.31-1, ANSI X9.42, ANSI X9.52, ANSI X9.55, ANSI X9.57, ANSI X9.62, ANSI X9.63, ANSI X9.73, ANSI X9.95, ETSI TS 101 733, ETSI TS 101 861, ETSI TS 101 862, ETSI TS 102, ETSI TS 133 310 (3GPP CMP), FIPS PUB 46-2, FIPS PUB 46-3, FIPS PUB 74, FIPS PUB 81, FIPS PUB 113, FIPS PUB 180, FIPS PUB 180-1, FIPS PUB 186, FIPS PUB 198, ISO/IEC 8372, ISO/IEC 8731 ISO/IEC 8732, ISO/IEC 8824/ITU-T X.680, ISO/IEC 8825/ITU-T X.690, ISO/IEC 9797, ISO/IEC 10116, ISO/IEC 10118, ISO/IEC 15782, ISO/IEC 18014, ITU-T X.842, ITU-T X.843, NSA Suite B, PKCS #1, PKCS #3, PKCS #5, PKCS #7, PKCS #9, PKCS #10, PKCS #11, PKCS #15, RFC 1319, RFC 1320, RFC 1321, RFC 1750, RFC 1991, RFC 2040, RFC 2104, RFC 2144, RFC 2202, RFC 2246, RFC 2268, RFC 2311, RFC 2312, RFC 2313, RFC 2314, RFC 2315, RFC 2437, RFC 2440, RFC 2459, RFC 2510, RFC 2511, RFC 2528, RFC 2560, RFC 2585, RFC 2630, RFC 2631, RFC 2632, RFC 2633, RFC 2634, RFC 2785, RFC 2876, RFC 2898, RFC 2984, RFC 2985, RFC 2986, RFC 3039, RFC 3058, RFC 3114, RFC 3126, RFC 3161, RFC 3174, RFC 3183, RFC 3211, RFC 3218, RFC 3261, RFC 3268, RFC 3274, RFC 3278, RFC 3279, RFC 3280, RFC 3281, RFC 3369, RFC 3370, RFC 3447, RFC 3546, RFC 3526, RFC 3565, RFC 3739, RFC 3770, RFC 3779, RFC 3851, RFC 3852, RFC 4055, RFC 4086, RFC 4108, RFC 4134, RFC 4210, RFC 4211, RFC 4231, RFC 4250, RFC 4251, RFC 4252, RFC 4253, RFC 4254, RFC 4256, RFC 4262, RFC 4279, RFC 4325, RFC 4334, RFC 4346, RFC 4366, RFC 4387, RFC 4419, RFC 4476, RFC 4492, RFC 4648, RFC 4680, RFC 4681, RFC 4853, RFC 4880, RFC 4945, RFC 5035, RFC 5055, RFC 5083, RFC 5246, RFC 5280, RFC 5288, RFC 5289, RFC 5430, RFC 5480, RFC 5652, RFC 5746, RFC 5750, RFC 5751, RFC 5753, RFC 5754, RFC 5756, RFC 5758, RFC 5816, RFC 5911, RFC 5912, RFC 6211, RFC 7539, RFC 7905, RFC 8439**