CTR\_DRBG

CTR\_DRBG 는 counter mode 내의 승인된 블록 암호화 알고리즘에 기반하여 작성되었다. (SP800-38A). 현재 3개의 키의 TDEA와 AES가 연방정부로부터 DRBG 메커니즘에 사용되는 것이 허용되었다. 난수 발생 결과들은 성공적인 숫자 값으로 암호화 되어 생성된다. 요구 값을 생성한 후에 새로운 키와 새로운 시작 카운터 값이 생성된다.

수행능력 : 대용량의 생성요구시 CTR\_DRBG는 다른 블록암호 알고리즘이 데이터를 암호화시키는 속도로 결과를 출력한다. 더욱이 CTR\_DRBG는 병렬로 처리된다. 각 생성 요구의 마지막에는 타 블록 암호 알고리즘에 근거하는 2, 3, 또는 4와 동등한 암호화가 수행되면서 새로운 키값과 카운터값이 다음 생성요구에 맞춰져 생성된다.

보안성 : CTR\_DRBG 의 보안성은 타 블록 암호알고리즘보다 우선한다 데 의의가 있고, 많은 숫자의 결과가 관찰되는 한, CTR\_DRBG에서의 어떠한 공격도 특정 블록암호알고리즘 상의 공격으로 표현한다.

결과의 제약 : 각각의 3개의 AES키 크기는 최대 까지 생성될 수 있다. 각각의 비트까지는 AES 상의 결점이 표현되지는 않는다. 그러나 작은 블록 크기의 TDEA 는 보다 많은 제약을 가지고 있다. 각각의 생성된 요구사항은 bit까지 제한되고, 대부분은 최대 으로 만들어진다.

자원 : CTR\_DRBG는 호출함수 없이 구현될 수 있다.

호출함수가 사용되면, CTR\_DRBG는 특정한 문자열을 처리할 수 있고 추가적인 입력은 DRBG 메커니즘과 같은 동일한 방법으로 할 수 있다. 그러한 구현은 어떠한 승인된 엔트로피 또는 전체 엔트로피에서 제공한 입력값의 자원입력으로 산출될 수 있다.

호출함수가 사용되지 않으면, CTR\_DRBG는 특정한 문자열과 추가적인 입력이 제공되면 보다 효율적이 될 수 있다. 그렇지만 틀정문자열의 길이와 추가입력이 seedlen 비트를 추가해서는 안된다. 그러한 구현은 전체 엔트로피가 제공하는 엔트로피의 입력에 의해 산출된다.

CTR\_DRBG는 키를 변화시키는 방법과 내부상태를 위한 저장공간을 포함한 블록암호알고리즘으로의 접근을 필요로 한다.

DRBG 메커니즘 기능들

DRBG의 메커니즘 함수들은 DRBG의 내부 상태로 처리된다. DRBG 메커니즘은 5개의 분리함수를 가지고 있다.

1. 예시된 함수는 엔트로피입력값을 얻어 그것을 초기 내부 상태가 생성된것으로 부터의 seed를 생생하기 위해 임시적이고 개별화된 문자열과 섞는다.
2. 생성함수는 요구사항에 근거한 난수 비트를 생성하는데 있어 현재 내부상태를 사용하고, 새로운 내부상태를 다음요구를 위해 생성한다.
3. Reseed 함수는 새로운 엔트로피 입력값을 필요로하고 그것은 현재 내부상태와 새로운 Seed와 새로운 내부상태를 위한 추가 입력 값과 결합한다.
4. 예시되지 않는 함수는 내부적으로 초기화된다.
5. 상태 체크 함수는 DRBG 메커니즘이 함수에서 지속되는지를 결정한다.

Seeds

DRBG가 난수비트를 생성하는데 사용될때, Seed는 DRBG에의해 출력비트의 생성에 앞서 얻어진다. Seed는 DRBG를 설명하는것과 초기 내부값을 결정하는데 사용된다.

Resseding은 seed 또는 내부상태가 알려질 때 DRBG의 출력의 기밀을 저장하는 수단으로 사용된다.

연속적인 reseeding은 DRBG seed의 위험요소를 찾는 좋은 방법이고, 엔트로피 입력또는 작업상태가 시간내내 중재되어진다. 어떤 기기(스마트카드)의 경우, 적절한 reseeding 절차가 가능하지 않을 수도 있다. 이러한 경우, 가장 좋은 방법은 프로세스 처리를 새로운 seed로 사용하는 DRBG로 대체하는 것이다.