Intel SGX:

* Erweiterung von Intel, die ab der 6. Generation von Intel-Core Prozessoren verfügbar ist (Codename Skylake, ab 2015)
* Ist im Bereich „hardware assisted security“ angesiedelt
* Problem was es versucht zu lösen:
  + Ausführung von Programmen auf einem System, auf dem jegliche privilegierte Software potentiell korrumpiert ist
  + Ausführung von Programmen auf Remotesystemen wie Cloud Computern, denen grundsätzlich nicht getraut werden kann, oder denen man nicht trauen will
* ... ohne dass vertrauliche Daten entblößt werden (Vertraulichkeit) oder Daten/Programmcode unwissentlich verändert wird (Integrität)
* die Folge ist, dass man anstatt dem auf dem Systen laufenden Betriebssystem oder dem Administrator, nur dem Intel Prozessor trauen muss, was man ohnehin machen muss
* Lösung dieser Probleme durch die Definition eines privaten Bereichs im Speicher (Speicherschema anmalen), der PRM genannt wird (Processor Reserved Memory)
* Dieser Bereich ist geschützt vor jeglichen Speicherzugriffen von außerhalb, inklusive der vom Kernel oder Hypervisor, etc.
* Innerhalb des PRM befinden sich die Enclaves, die wiederum komplett isolierte Speicherbereiche innerhalb des PRM darstellen (in der Praxis sind Enclaves eingebundene .dll Libraries)
* Die Ausführung von Code innerhalb der Enclaves ähnelt dabei einem Sprung vom user mode in den kernel mode