DFx Secure Plugin
Intel Corporation Soft IP

Overview

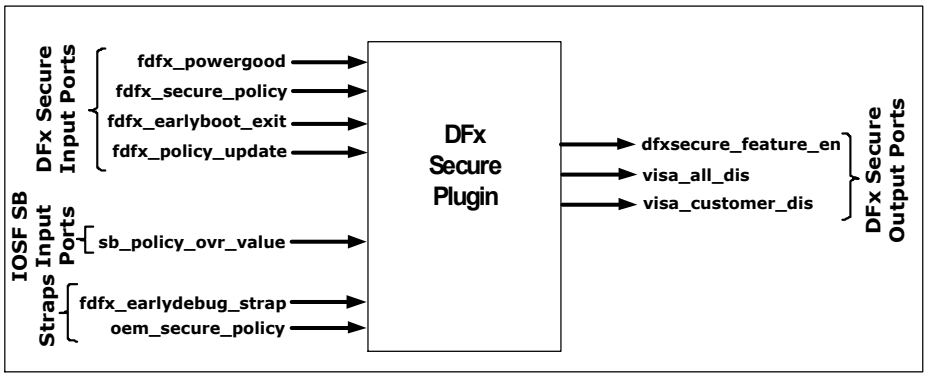
The DFx Secure Plugin IP is a soft IP that translates the current policy into a value that enables or disables access to DFx features from all IP blocks in the SoC.

It uses a DFx secure policy signal group composed of a binary encoded policy bus, a latch enable, and an early boot debug exit signal. This signal group is distributed from a centralized DFx security aggregator.

Features

- Translates the current policy and enables or disables access to DFx features within the agent or IP-block
- Supports HDK

IP Block Diagram



Major Interfaces

- **DFx Secure Input Ports:** This is the interface driven by the DFx Security Aggregator.

Applications

- DFx Security for features that need to be secured (such as VISA and TAP Test Data Registers)

Power and Performance Parameters

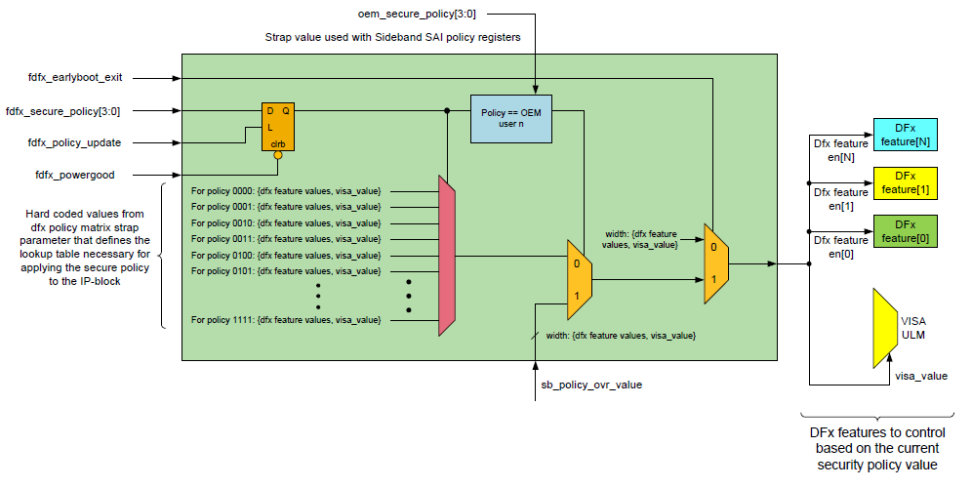
The following table shows the values for several area and power parameters based on the 1273 process.

Parameter Type	Value
Gate Count	35
Total Dynamic Power	1.022 mW
Leakage Power	6.985 nW

Deliverables

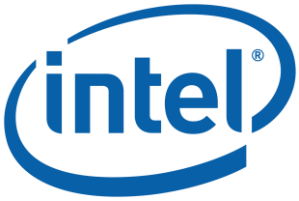
- Customer Documentation
- RTL
- Test cases, Cover points, and Assertions
- Testbench environment in Open Verification Methodology (OVM)
- Lintra, LEC, and Synthesis scripts
- Release Notes

SoC Integration & Related Products



Security Audits

This IP is exempt from all audits as this is the base IP where other IPs will set their security controls.



This document contains information on products in the design phase of development.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your Intel account manager or distributor to obtain the latest specifications and before placing your product order.

Copies of documents that have an order number and are referenced in this document or in other Intel literature can be obtained from your Intel account manager or distributor.