ChevinID© - Silicon Security Solution

Chevin Technology's ChevinID© is a Silicon Security Solution that offers an additional layer of protection against malicious and accidental changes to Silicon supply chains, using a patented method to authenticate and authorize Hardware and Software functions on Silicon devices. ChevinID© establishes a secure root of trust while allowing the selection, control and modification of features contained within encrypted envelopes of RTL netlists. ChevinID© can be inserted into Silicon such as FPGA, ASIC, and SiP design with Chiplets.

Features can be securely selected or modified dynamically, at power-up or during run-time. The ChevinID© solution is vendor agnostic, so adds security when using products from multiple vendors in FPGAs, ASICs or Chiplets. ChevinID© works with a server that can be located on an FPGA, on a CPU with secure/protected software, or cloud hosted, with an internet connection.

Key Features

- *Authenticate and Authorize Hardware or Software Functions*
- *Patented method prevents malicious or unintended changes*
- *Additional Layer of Protection for Silicon: FPGAs, ASICs, Chiplets*
- *Vendor independent software configuration management*
- *Securely select or modify features*
- *Flexible use rights management*
- *Single or multiple Client/Server*
- *Seamless integration with AXI4_MM Connectivity*
- *Supports multiple 3rd Party Software*
- *Optional Cloud located Server*

Benefits

- *Secure Root of Trust*
- *Protect against cyber hacks, copying, cloning, trojans*
- *Flexible management and Upgrade path for features*
- *Reduced complexity with software keys*
- *Control features to differentiate products, maximise revenue stream*

Markets

Defense · Aerospace · Cyber Security · Automotive · Telecoms · Broadcast · Data Centre · Wearables · Scientific · Medical ·

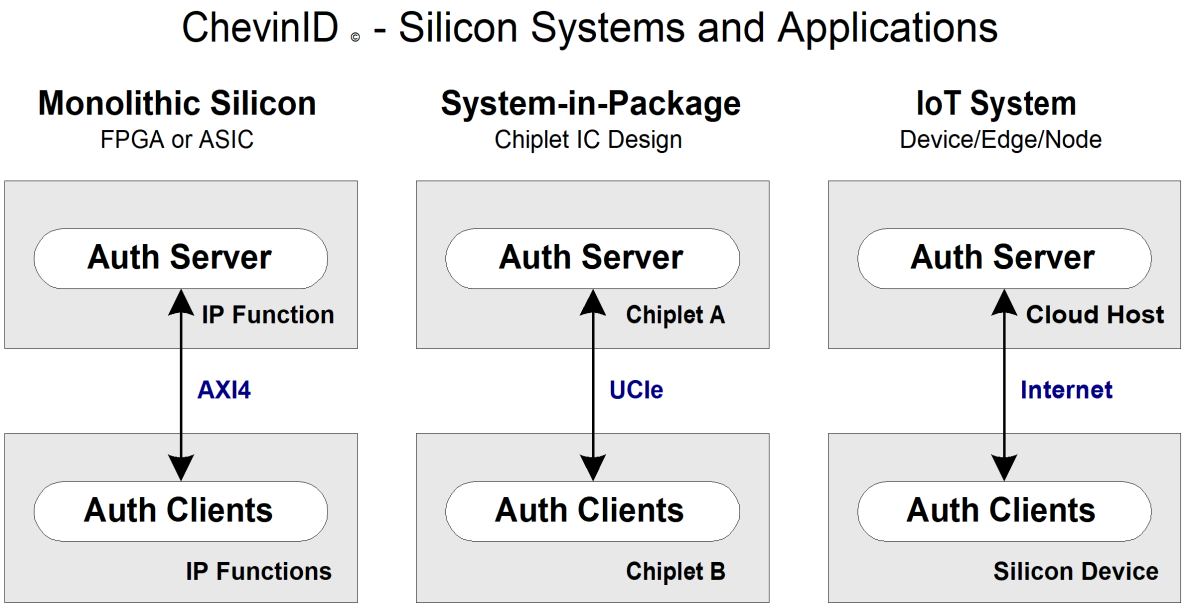
Chevin Technology Ltd., The Bradfield Centre, 184 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire, CB4 0GA
Telephone: +44 (0)1223 817009 Email: ip@chevintechnology.com www.chevintechnology.com

ChevinID© - Silicon Security Solution

The Solution

Many Software applications today contain multiple IP blocks from several different vendors, exposing the complex Silicon supply chain to threats and vulnerabilities. Chevin Technology's ChevinID© authentication provides a secure solution to protect Hardware, Software & Licenced Materials, by identifying and authorising the authentic hardware. Each hardware silicon fabric is uniquely identified by a Physically Unclonable Function (PUF), such as the CHIP_ID, DNA_PORT identifier, or a softcore PUF function. Private keys are kept within the encrypted envelope of the protected block, such as an IP RTL-netlist, OTP fuse memory for ASIC, an encrypted FPGA bitfile or a compiled and encrypted embedded software binary file.

ChevinID© uses a server/client model where the server, containing the PUF, such as DNA_PORT, CHIP_ID, and a secret random number such as an OTP antifuse in silicon or a constant programmed in silicon, contains a list of features that can be selected at run-time by programming the associated key. The Server location can be on chip, off-chip or remotely located off-site via an internet connection. The Client can request and manage features from the feature list located in the Server. The Server ensures that only genuine Clients are permitted to run the requested feature, by computing messages and returning responses to its Clients at regular intervals. In addition to authenticating genuine silicon, ChevinID© also provides a convenient way to dynamically select features, differentiate products and drive revenue growth.



Chevin Technology Ltd., The Bradfield Centre, 184 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire, CB4 0GA
Telephone: +44 (0)1223 817009 Email: ip@chevintechnology.com www.chevintechnology.com