Licence Management System

CT1002-LMS - Product Brief - Version 1.1– 23rd January 2023

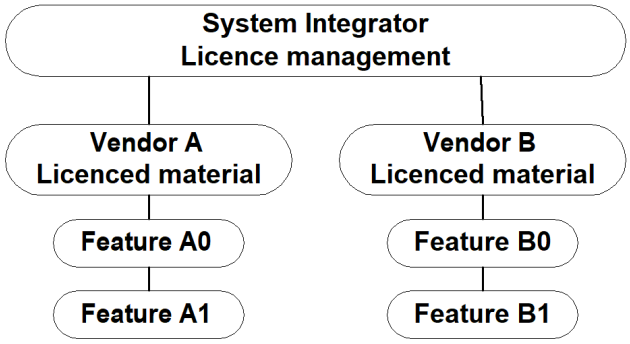
Overview

Chevin Technology's Licence Management System uses a patent pending method to authenticate and authorize software features in IP functions. The system provides a secure way to select and modify features contained within encrypted envelopes of RTL netlists from one or more vendors. Features can be selected or modified dynamically, at power-up or during run-time.

The licence management system is vendor independent and can protect IP from multiple sources in one or more physical devices. The licence management system works with a client and server that can be located on an FPGA, on a CPU with secure/protected software, or cloud-hosted with an internet connection.

Key Benefits

- *Vendor independent licence management*
- *Reduce Risk of cyber hacks, copying, cloning*
- *Flexible Upgrade path for features*
- *Reduced complexity with software keys*
- *Improved software config management*



Key Features

- *Authenticate and Authorize Software Functions*
- *Securely select or modify features*
- *Licence Key for flexible use rights management*
- *Single or multiple Client/Server*
- *Seamless integration with AXI4_MM Connectivity*
- *Supports multiple vendor's IP with single server*
- *Message analysis statistics collection*
- *Small footprint, Server 3k7 LUTs, Client 2k1 LUTs*
- *Client/Server messaging over standard AXI4_MM*
- *Optional Cloud located Server*
- *Patent pending, patent applications filed in USA, Europe & UK*

Performance Figures

Licence features (# of)	Unlimited
Vendors (# of)	Unlimited
Keys (# of)	Unlimited
Licence Validation Time	< 1 ms
Licence Dynamic re-config	< 1 ms

Location server/client	On-chip (AXI4MM)
	Off-chip (SW)
	Off-site (internet)
Auth_servers (# of)	Single or Quorum
Auth_clients (# of)	Single or Multiple

ETHERNET PROTOCOLS

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

The Technology

Many applications today contain multiple IP blocks from several different vendors. This system provides a secure and flexible way to protect licenced materials, by locking its use to a name physical hardware, also known as a hardware-lock or node-lock.

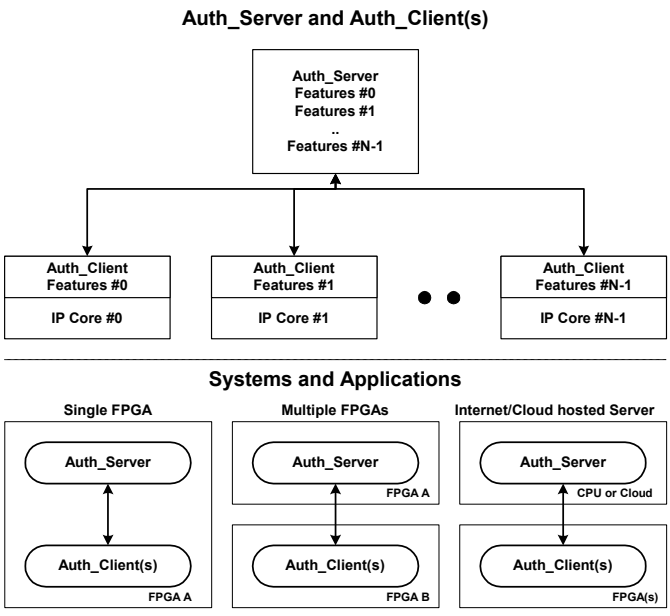
Each hardware silicon fabric is uniquely identified by a Physically Unclonable Function, such as the DNA_PORT (eFUSE) identifier, external SHA1 device or a softcore PUF function. Each vendor is given a unique secret key that is kept within the encrypted envelope of the protected block, for example an IP RTL-netlist, an encrypted FPGA bitfile or a compiled and encrypted embedded software binary file. A vendor selects the features to be enabled and produces an authorization key that is shared with the customer and controls the way features can be allowed to run inside the block. This could be increased compute capability, different storage method, or for example a time limited evaluation to run only on a single dedicated board. It could be a general upgrade of capabilities to be rolled out over thousands of products. The vendor can therefore develop and deliver software with maximum capabilities built-in, and then selectively enable features based on different keys authorizing features, rather than doing so with differently built software versions. The authorization keys themselves are not secret, and can be administered easily by means of embedded software such as the customers own system software or obtained over an internet connection.

The Server Client model

Auth clients communicate with an Auth server, each node securely contained within an encrypted envelope. The client or server node location can be on chip, off-chip or remotely located off-site via an internet connection. In an FPGA the communication between the Auth_client and Auth_server uses the Avalon or AXI4_MM interconnect. Messages are periodically exchanged between the server and client to determine licence status and obtain permission to run features as defined by a vendor. All the functionality required to run is contained within the client and server blocks, and can be configured to run as HDL or software processes on an embedded CPU.

FPGA Applications

The management system can be run on any FPGA with Xilinx DNA_PORT/eFUSE or Intel CHIP_ID, and be used to protect code in one or more FPGAs for each system.



Deliverables

- Encrypted compiled netlist
- Datasheet & User Guide
- Reference Designs
- Simulation Test bench
- Build scripts for Vivado
- Support for integration into FPGA

FPGA Resource Figures

Auth Server 3750 LUTs

Auth Client 2100 LUTs

Memory Footprint 1 BRAM

Options: FPGA/RTL, CPU/SW , Cloud

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