# MachXO3D Security Checklist

# Technical Note

FPGA-TN-02311-1.1

April 2023

## Disclaimers

Lattice makes no warranty, representation, or guarantee regarding the accuracy of information contained in this document or the suitability of its products for any particular purpose. All information herein is provided AS IS, with all faults and associated risk the responsibility entirely of the Buyer. Buyer shall not rely on any data and performance specifications or parameters provided herein. Products sold by Lattice have been subject to limited testing and it is the Buyer's responsibility to independently determine the suitability of any products and to test and verify the same. No Lattice products should be used in conjunction with mission- or safety-critical or any other application in which the failure of Lattice's product could create a situation where personal injury, death, severe property or environmental damage may occur. The information provided in this document is proprietary to Lattice Semiconductor, and Lattice reserves the right to make any changes to the information in this document or to any products at any time without notice.

# Contents

# Tables

# Acronyms in This Document

A list of acronyms used in this document.

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EFB | Embedded Function Block |
| ESB | Embedded Security Block |
| GUI | Graphic User Interface |
| HSM | Hardware Security Module |
| JEDEC | Joint Electron Device Engineering Council |
| NDA | Non-disclosure Agreement |
| OTP | One-time Password |
| SPI | Serial Peripheral Interface |
| UFM | User Flash Memory |

# 1. Introduction

Security is a rising concern with new systems. MachXO3D™ devices feature cryptographic functions that help secure the systems. This technical note summarizes all the security-related features in MachXO3D devices, which cover from initial Diamond software setup for security functions, critical security requirements related to MachXO3D devices during the provisioning/programming stage (bitstream security, lock policy for ports, function, etc.) as well as user mode security functions managed by Embedded Security Block. It does not provide detailed step-by-step instructions but offers a high-level summary of security functions.

This technical note assumes that the reader is familiar with the MachXO3D device features as described in the MachXO3D Family Data Sheet (FPGA-DS-02026).

The critical security areas covered in this technical note include:

- Enabling MachXO3D device security settings in Lattice Diamond® software
- Enabling bitstream security settings in the Diamond Security Setting tool
- Security key programming for bitstream authentication and encryption in Lattice Diamond Programmer
- Bitstream authentication/signing with HSM generated signature
- MachXO3D device lock policy for ports and assets
- User mode security functions covered by Embedded Security Block
- Tamper detection feature in MachXO3D
- SupplyGuard for MachXO3D devices

## 1.1. Reference Documents

Refer to the following documents for detailed recommendations:

- MachXO3D Programming and Configuration Usage Guide (FPGA-TN-02069)
- Using Hardened Control Functions in MachXO3D Devices (FPGA-TN-02117)
- Using Hardened Control Functions in MachXO3D Devices Reference Guide Supplement (FPGA-TN-02241)
- Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)*
- MachXO3D Embedded Security Block (FPGA-TN-02091)*
- Tamper-Detection-Response-for-MachXO3D-Devices (FPGA-TN-02143)*
- Signing JEDEC with HSM-Generated Signature (FPGA-TN-02260)*
- HSM Platform Agnostic EPP Generation and Programming (FPGA-TN-02243)*
- SupplyGuard Architecture Overview (FPGA-TN-02304)*
- SupplyGuard Portal User Guide (FPGA-UG-02144)*

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information**.**

# 2. Lattice Diamond Software

Lattice Diamond software requires an encryption pack to enable security features. The encryption pack enables security features for user primitives (authentication and encryption) on MachXO3D devices. After installing the Lattice Diamond software successfully, download the encryption pack from the Lattice Semiconductor website.

# 3. Bitstream Security Settings

Users can enable flash protection passwords for read/write lock access, authentication, and encryption in the configuration bitstream. All the MachXO3D device bitstream security options can be accessed using the Bitstream security settings Graphic User Interface (GUI) in the Lattice Diamond software.

Flash Protection Password:

- MachXO3D offer 128-bit password protection for device configuration access, which user can optionally enable
- The password security feature utilizes a Flash Protect Key to provide a method of controlling access to the configuration and programming modes of the device
- Write, Verify, and Erase operations are allowed only when presented with a Flash Protect Key which matches that stored in the device.

**Table 3.1. Authentication and Encryption on the Bitstream**

| Security Protocol | Encryption (AES-256) | Authentication (ECDSA) | Bitstream Format |
|---|---|---|---|
| AES Encryption | Yes, AES Key | No | Encrypted Bitstream |
| Authentication (ECDSA) | No | Yes, ECDSA private and public key | Plain bitstream + Signature generated using ECDSA private key |
| Authentication (ECDSA) and AES Encryption | Yes, AES Key | Yes, ECDSA private and public key | AES Encrypted data (Plain bitstream + Signature generated using ECDSA private key) |

- Refer to MachXO3D Embedded Security Block (FPGA-TN-02091)* - Bitstream Security Chapter for more details on how to enable security settings on bitstream.
- Refer to the Device Bring Up Examples section of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* for some overall use case examples.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information**.**

# 4. Bitstream Authentication

MachXO3D devices support ECDSA-based authentication. Public key can be programmed into the device through Diamond Programmer to enable authentication for prototyping purposes. For details on how to program the public key, refer to the Device Bring Up Examples (Section 5.4.3) of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* for public key programming.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information**.**

As for Production environment, HSM is recommended to be used as secure applications for authentication enablement. Openssl can be used to generate ECDSA key pair and signature, while two python scripts are provided by Lattice Semiconductor to extract digest and replace signature in the bitstream, with the flow demonstrated below:

1. Generate dummy signed FPGA bitstream using Lattice Diamond Software – Security Settings tool.
    a. Use the Lattice Diamond Software to generate a signed FPGA bitstream (JEDEC file). The signed bitstream has signature embedded in it. The signature in this setup is generated using an auto key pair using Security settings tool as a place holder for signature in the JEDEC file.
2. Get the keys ready.
    a. For secure applications, generate a key pair from HSM.
3. Source Lattice provided Reference Python scripts.
    a. There are two python scripts:
        i. One is used to extract the configuration data from bitstream, which is used for generating signature;
        ii. The other one is used to replace the existing signature with the actual signature generated from HSM.
4. Program the Public key and signed bitstream (JEDEC file) into MachXO3D FPGA.

For details on how to enable the HSM signing flow, refer to Signing JEDEC with HSM-Generated Signature (FPGA-TN-02260)*.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information**.**

In addition, public key sector (PUBKEY) can be secured with one-time password (OTP) to avoid any further updates to this public key. The PUBKEY sector has three lock policies: Erase lock, Write/Program lock, and Read lock. The PUBKEY sector has three lock policies: Erase lock, Write/Program lock, and Read lock. Table 4.1 summarize the PUBKEY memory access policy settings available for user to choose:

**Table 4.1. PUBKEY Memory Access Policy Settings**

| Diamond Programmer Option | Description |
|---|---|
| Read Lock | When enabled, the read access to PUBKEY is locked (soft-locked). This is an OTP operation, in which PUBKEY is always locked unless unlocked by user through Wishbone access. If Hard Lock (disable Wishbone access) is required, user needs to turn on this option together with “Lock Wishbone Access (Hard Lock)” option. |
| Write Lock | When enabled, the write/program access to PUBKEY is locked (soft-locked). This is an OTP operation, in which PUBKEY is always locked unless unlocked by user through Wishbone access. If Hard Lock (disable Wishbone access) is required, user needs to turn on this option together with “Lock Wishbone Access (Hard Lock)” option. |
| Erase Lock | When enabled, the erase access to PUBKEY is locked (soft-locked). This is an OTP operation, in which PUBKEY is always locked unless unlocked by user through Wishbone access. If Hard Lock (disable Wishbone access) is required, user needs to turn on this option together with “Lock Wishbone Access (Hard Lock)” option. |
| OTP | Turning on this option to similar as enabling Write Lock and Erase lock. |
| Lock Wishbone Access (Hard Lock) | Turn on this option if user wishes to block Wishbone access for any unlock operation. This option needs to be turned on together with one or more options from Read/Write/Erase lock. |

- For details on how to enable OTP settings, refer to the Device Feature and Security Programming sections of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)*.
- For details on how to unlock memory access through Wishbone, refer to the Lock Altering Through WISHBONE Interface sections of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)*.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.*

# 5. Bitstream Encryption

MachXO3D devices support AES encryption. AES key can be programmed into the device through Diamond Programmer to enable encryption. For details on how to program the AES key, refer to the Device Bring Up Examples – Program the AES Encryption Key section of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* for AES key programming.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.*

In addition, AES key sector (AESKEY) can be secured with one-time password (OTP) to avoid any further updates to this AES key. The AESKEY sector has three lock policies: Erase lock, Write/Program lock, and Read lock. Table 5.1 summarizes the AESKEY memory access policy settings available for user to choose:

**Table 5.1. AESKEY Memory Access Policy Settings**

| Diamond Programmer Option | Description |
|---|---|
| Read Lock | When enabled, the read access to AESKEY is locked (soft-locked). This is an OTP operation, in which AESKEY is always locked unless unlocked by user through Wishbone access. If Hard Lock (diable Wishbone access) is required, user needs to turn on this option together with “Lock Wishbone Access (Hard Lock)” option. |
| Write Lock | When enabled, the write/program access to AESKEY is locked (soft-locked). This is an OTP operation, in which AESKEY is always locked unless unlocked by user through Wishbone access. If Hard Lock (disable Wishbone access) is required, user needs to turn on this option together with “Lock Wishbone Access (Hard Lock)” option. |
| Erase Lock | When enabled, the erase access to AESKEY is locked (soft-locked). This is an OTP operation, in which AESKEY is always locked unless unlocked by user through Wishbone access. If Hard Lock (disable Wishbone access) is required, user needs to turn on this option together with “Lock Wishbone Access (Hard Lock)” option. |
| OTP | Turning on this option is similar to enabling Write Lock and Erase lock. |
| Lock Wishbone Access (Hard Lock) | Turn on this option if user wishes to block Wishbone access for any unlock operation. This option needs to be turned on together with one or more options from Read/Write/Erase lock. |

- For details on how to enable OTP settings, refer to the Device Feature and Security Programming sections of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)*.
- For details on how to unlock memory access through Wishbone, refer to the Lock Altering Through WISHBONE Interface section of the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)*.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.*

Optionally, users are allowed to enable clock randomization and background noise when users program the AES key to mitigate side channel attack. Besides, user can choose to enable “Encrypted Bitstream Only” mode if unencrypted bitstream is prohibited from loading into the device.

# 6. Protecting Data in Assets

Assets are the different flash sectors in MachXO3D devices. Besides the PUBKEY and AESKEY sectors discussed earlier, there are another 10 flash sectors, made up total of 12 flash sectors shown in Table 6.1. Same lock policies (read, write, and erase lock) apply to all the flash sectors.

Each flash sector has its own local lock and central lock. In local locking scheme, users can enable/disable memory access (program and read operations) to all flash sectors by selecting the appropriate flash sector and enabling the local security bit for that sector. On the other hand, in central locking scheme, the memory accesses (erase and read specifically) to the CFG, UFM, Feature, and Security Keys flash sectors are controlled by setting appropriate bits in the centralized security settings flash sector.

**Table 6.1. Memory Access and Central Bits Location of Flash Sectors**

| Flash Sector/SRAM | Memory Access | | | Central Bits Location |
|---|---|---|---|---|
| | Erase | Read | Program | |
| **CFG/Feature/Security Keys/SRAM** | | | | |
| CFG0 | Central | Central/Local | Local | CSEC |
| CFG1 | Central | Central/Local | Local | |
| FEA | Central | Central/Local | Local | |
| PUBKEY | Central | Central/Local | Local | |
| AESKEY | Central | Central/Local | Local | |
| SRAM | Central | Central/Local | Local | |
| **UFM** | | | | |
| UFM0 | Central | Central/Local | Local | USEC |
| UFM1 | Central | Central/Local | Local | |
| UFM2 | Central | Central/Local | Local | |
| UFM3 | Central | Central/Local | Local | |
| **Central/User Security Settings** | | | | |
| CSEC | Local | Local | Local | N/A |
| USEC | Local | Local | Local | N/A |

Refer to the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* - Memory Access section for available settings to enable/disable locks.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.

The locking feature adds a layer of protection on top of the existing authentication and encryption features. OTP is recommended if User Flash Memory (UFM) contains critical data.

## 6.1. Updating Data in Assets

Use soft locks to allow data updates in the future.

- To modify soft locks, use the internal wishbone interface.

**Note**: Critical data, such as all keys (public key, encryption key), should be hard-locked and OTP protected to prevent further updates.

Refer to the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* - Fixed Lock versus Dynamic Lock & Lock Policy Settings and Lock Bits Description sections for details about the various locking options available in MachXO3D devices.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.

# 7. Port Locking

The port access is used to control access to the external configuration ports of MachXO3D devices. These configuration ports can either be partially or totally locked. To provide finer control of instructions/commands that are used to access MachXO3D device, port locking can be further expanded into 4 lock modes to provide finer control of instructions/commands. Refer to Lock Policy and Access Types section in Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)*.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.

Table 7.1 summarizes the locking mechanism for all 5 types of configuration ports in MachXO3D devices.

**Table 7.1. Locking Mechanism of Configuration Ports**

| Port Access | Hard Lock | Locking Mechanism | |
|---|---|---|---|
| | | Partial Lock | Total Lock |
| JTAG | Supported | Supported | Supported |
| Slave SPI | Supported | Supported | Supported |
| Slave I2C | Supported | Supported | Supported |
| JTAG to SPI Bridge | Supported | N/A | Supported |
| I2C Bridge | Supported | N/A | Supported |

- Refer to the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* - Port Access Section for details about port locking mechanism in MachXO3D.
- Refer to the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* - CEG Port Lock Option Programming section for details about port locking OTP programming guide.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.

# 8. User Mode Security Function

To establish Root of Trust or better security control on the device during user mode, the hardened control functions in the Embedded Function Block (EFB) can be utilized in user design in order to perform read/write on internal flash sectors. Tamper Detection feature can be enabled by configuring the EFB module to enable Tamper Detection/Response. Once enabled, this tamper is continuously monitoring the activity on external configuration ports as well as memory access (Flash sector and SRAM).

Apart from EFB, as per the soft-lock mechanism, users need to ensure there is an unlock/lock algorithm implemented in the core fabric design if soft-lock is needed for port locking or memory access lock.
The MachXO3D device offers a suite of enhanced security algorithms and features, including 128-bit/256-bit Advanced Encryption Security (AES-128/AES-256), 256-bit Secure Hash Algorithm (SHA256), and Elliptic Curve Digital Signature Algorithm (ECDSA), which are essential for security-sensitive applications. These advanced security functions are realized by utilizing the Embedded Security Block (ESB) integrated into the MachXO3D device. The ESB incorporates multiple security blocks used for authentication and configuration functions. To leverage these advanced security functions, users can incorporate the ESBA Primitive into their design.

- Refer to the Using Hardened Control Functions in MachXO3D Devices Reference Guide (FPGA-TN-02119)* for details about EFB.
- Refer to the Tamper Detection/Response for MachXO3D Devices (FPGA-TN-02143)* for details about Tamper Detection on MachXO3D devices.
- Refer to the MachXO3D Embedded Security Block (FPGA-TN-02091)* for details about all the security features supported by MachXO3D ESB.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information.

# 9. SupplyGuard for MachXO3D Devices

SupplyGuard is an end-to-end supply chain protection service for MachXO3D devices to ensure ownership transfer can be carried out securely. This technology preserves trust throughout the dynamic supply chain at the lowest cost by providing protection against supply chain attacks such as spoofing, cloning, counterfeiting, trojan insertion, tampering during transit, and overbuilding.

Refer to the following technical notes for details about SupplyGuard in MachXO3D devices:

- SupplyGuard Architecture Overview (FPGA-TN-02304)*
- HSM Platform Agnostic EPP Generation and Programming (FPGA-TN-02243)*
- SupplyGuard Portal Userguide (FPGA-UG-02144)*

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information**.**

# 10. Device Bring-up Use Case Examples

There are five different MachXO3D device use cases describing how to enable dual boot, authentication, encryption, and different locking options. Refer to the Lock-Policy-Settings-for-MachXO3D-Devices (FPGA-TN-02132)* - General Device Setup Cases section for details. These are common use cases and there can be many different combinations and permutations based on specific implementation.

***Note:** Access to this technical note requires a Non-disclosure Agreement (NDA). Contact Lattice Semiconductor marketing team for more information**.**

# 11. Licenses

The following license feature lines are required to enable bitstream security and user mode security features in MachXO3D devices:

- To enable bitstream security (authentication and encryption) - LSC_SW_XO3D_SECURITY_ENCRYPT
- To enable Embedded Security Block (ESBA) user primitive - LSC_SW_XO3D_HARDIP_ESBA

To enable MachXO3D device locking features - LSC_SW_XO3D_SECURITY_LOCK

# 12. Checklist

Table 12.1 lists the MachXO3D security checklist items.

**Table 12.1. MachXO3D Security Checklist Items**

| S. No. | MachXO3D Security Checklist Items | Status | N/A |
|---|---|---|---|
| 1 | Prerequisite | | |
| 1.1 | Diamond Software | | |
| 1.2 | Encryption Pack | | |
| 1.3 | License | | |
| 2 | Configuration Security | | |
| 2.1 | Bitstream Security Settings | | |
| 2.2 | Keys Provisioning/Programming – Flash Protection Key, Public key, AES key | | |
| 2.3 | Memory Access Lock Policy | | |
| 2.4 | Port Locking | | |
| 3 | User Mode Security | | |
| 3.1 | EFB and Tamper Detection | | |
| 3.2 | Lock/Unlock Algorithm for Soft-lock policy | | |
| 3.3 | Security Function by ESB | | |
| 4 | Supply Chain Security | | |
| 4.1 | SupplyGuard Solution | | |

# Technical Support Assistance

Submit a technical support case through www.latticesemi.com/techsupport.

For frequently asked questions, refer to the Lattice Answer Database at www.latticesemi.com/en/Support/AnswerDatabase.

# Revision History

**Revision 1.1, April 2023**

| Section | Change Summary |
|---|---|
| Acronyms in This Document | Added the following Acronyms: AES, ECDSA, EFB, ESB, HSM, JEDEC, and SPI. |
| Introduction | • Revised critical security areas covered in this technical note.<br>• Added 'SupplyGuard Architecture Overview (FPGA-TN-02304)' as a reference document in the Reference Documents section. |
| Bitstream Security Settings | • Revised to add ‘Flash Protection Password’ details.<br>• Added Table 3.1. Authentication and Encryption on the Bitstream. |
| Bitstream Authentication | • Revised to add 'Public Key Programming' details.<br>• Added Table 4.1. PUBKEY Memory Access Policy Settings. |
| Bitstream Encryption | • Revised to add 'AES Key Programming' details.<br>• Added Table 5.1. AESKEY Memory Access Policy Settings. |
| Protecting Data in Assets | • Revised to add 'Flash Sectors' details.<br>• Added Table 6.1. Memory Access and Central Bits Location of Flash Sectors. |
| Port Locking | Added Port Locking section. |
| User Mode Security Function | Added User Mode Security Function section. |
| Checklist | Added Checklist section. |
| Technical Support Assistance | Added reference link to the Lattice Answer Database. |

**Revision 1.0, July 2022**

| Section | Change Summary |
|---|---|
| All | Initial release. |


www.latticesemi.com