lenovo
NEW WORLD. NEW THINKING.

ThinkPad BIOS Password Design for UEFI

Mikio Hagiwara

BIOS Development
TVT & Notebook SW Development
Technical Operations

Design Concept

- Comply with UEFI spec version 2.3 section 31 User Identification
- Extensible to support credential providers such as fingerprint readers, Smart Card readers, the HPM User Login, WOL packets and so on
- Inherit legacy password architecture

Major changes

- Passphrase mode is always enabled. Never disabled
- Resume password prompt is not supported
- Internal password data length is extended to 16 bytes

Password Characteristics

Password Characters and Data

- Supported characters
  - Alphabet (case insensitive)
  - Number
  - Space ‘ ‘
- Code set
  - Scan code
- Maximum length
  - 64 characters
- Data transformation
  - Hash 64 scan codes by SHA-256 and take first 16 bytes

Power On Password

- Requested to input at:
  - Boot
  - Waking up from Hibernate (POST)

- Storage
  - CMOS

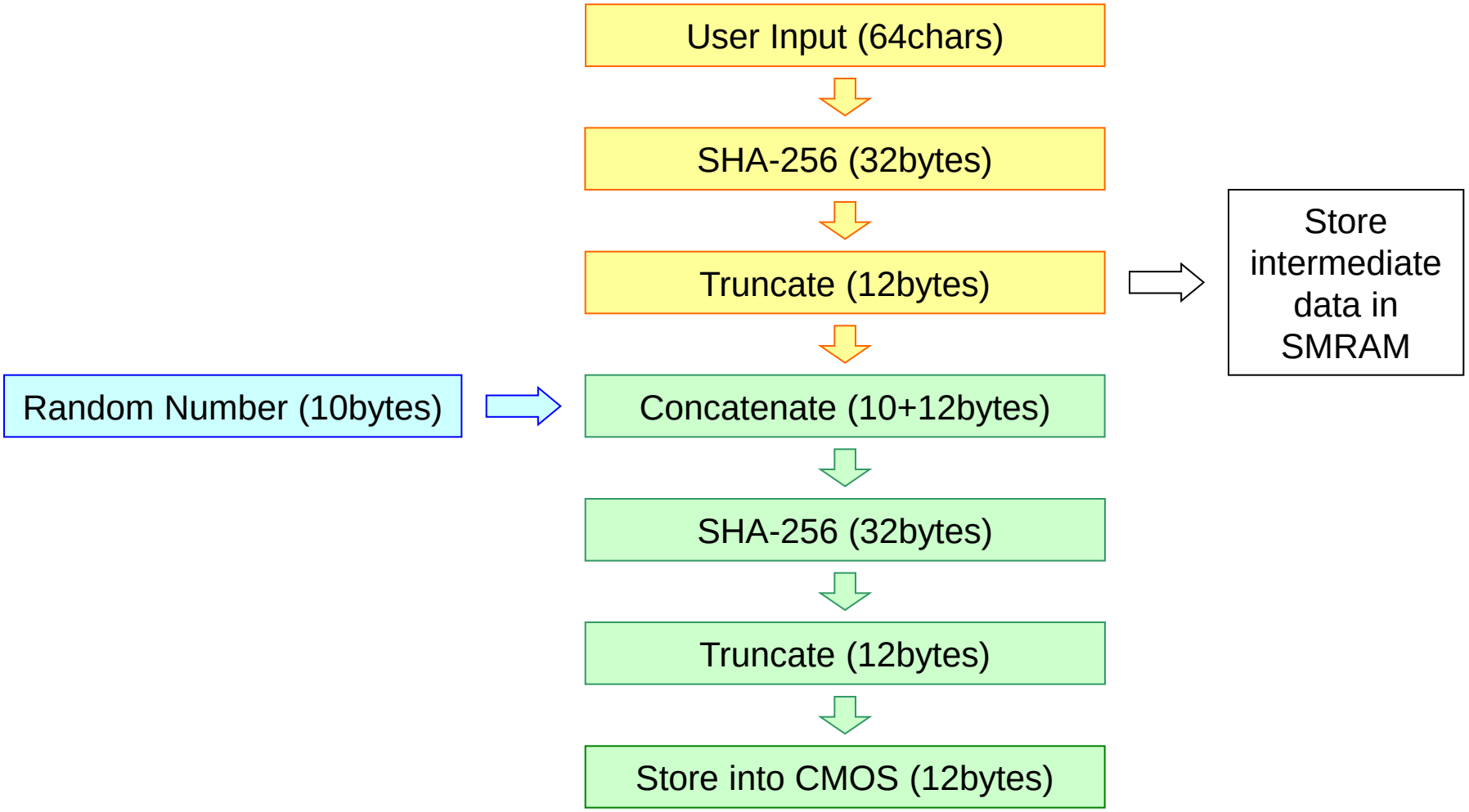
    Lower 38-3Fh : First 8bytes of hashed passphrase (Offset 0-7h)
    Upper 38-3Bh : Remaining 4bytes of hashed passphrase (Offset 8-Bh)
    Upper 3Ch : Checksum of lower 38-3Fh and upper 38-3Bh

  - Storage are locked
    - before exiting POST if the signature diskette is not detected
    - before jumping to OS waking vector

- Salting
  - Salted with the random number in the boot block before storing in the CMOS

- POP is used to unlock User HDP
  - Boot
  - Resuming from S4

Power On Password generation flow



Supervisor Password

- Requested to input when:
  - BIOS Setup is invoked
  - Signature diskette is detected
  - EFI Shell is invoked
  - BIOS update is invoked while OS is running
  - TPM state change is invoked while OS is running

- Storage
  - EEPROM Block 6 (C2 Space)

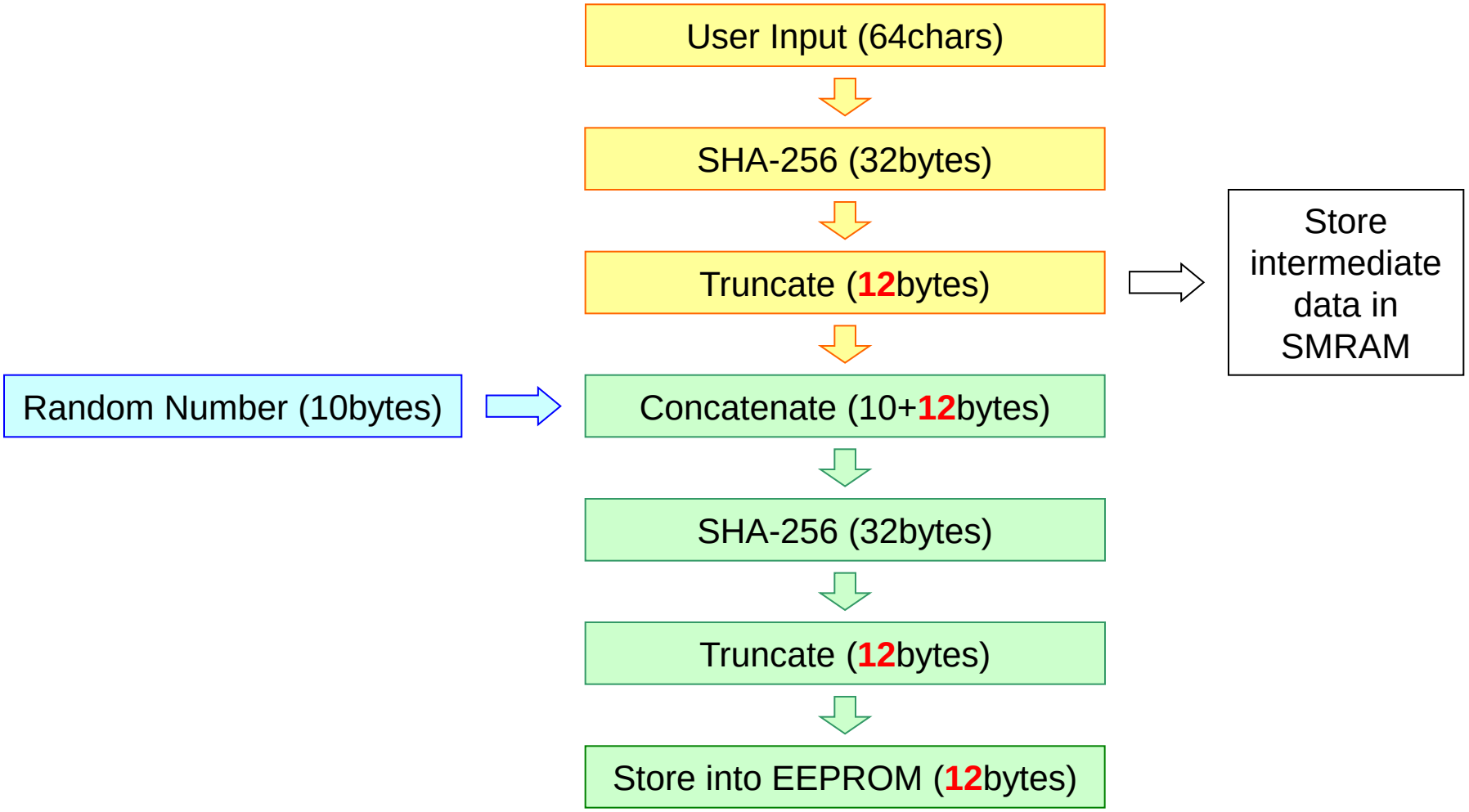
    10-1Fh : Primary SVP
    20-2Fh : Backup SVP

  - Storage are locked
    - before exiting POST if the signature diskette is not detected
    - before jumping to OS waking vector

- Salting
  - Salted with the random number in the boot block before storing in the EEPROM

- SVP can be used as alternative of POP

Supervisor Password generation flow



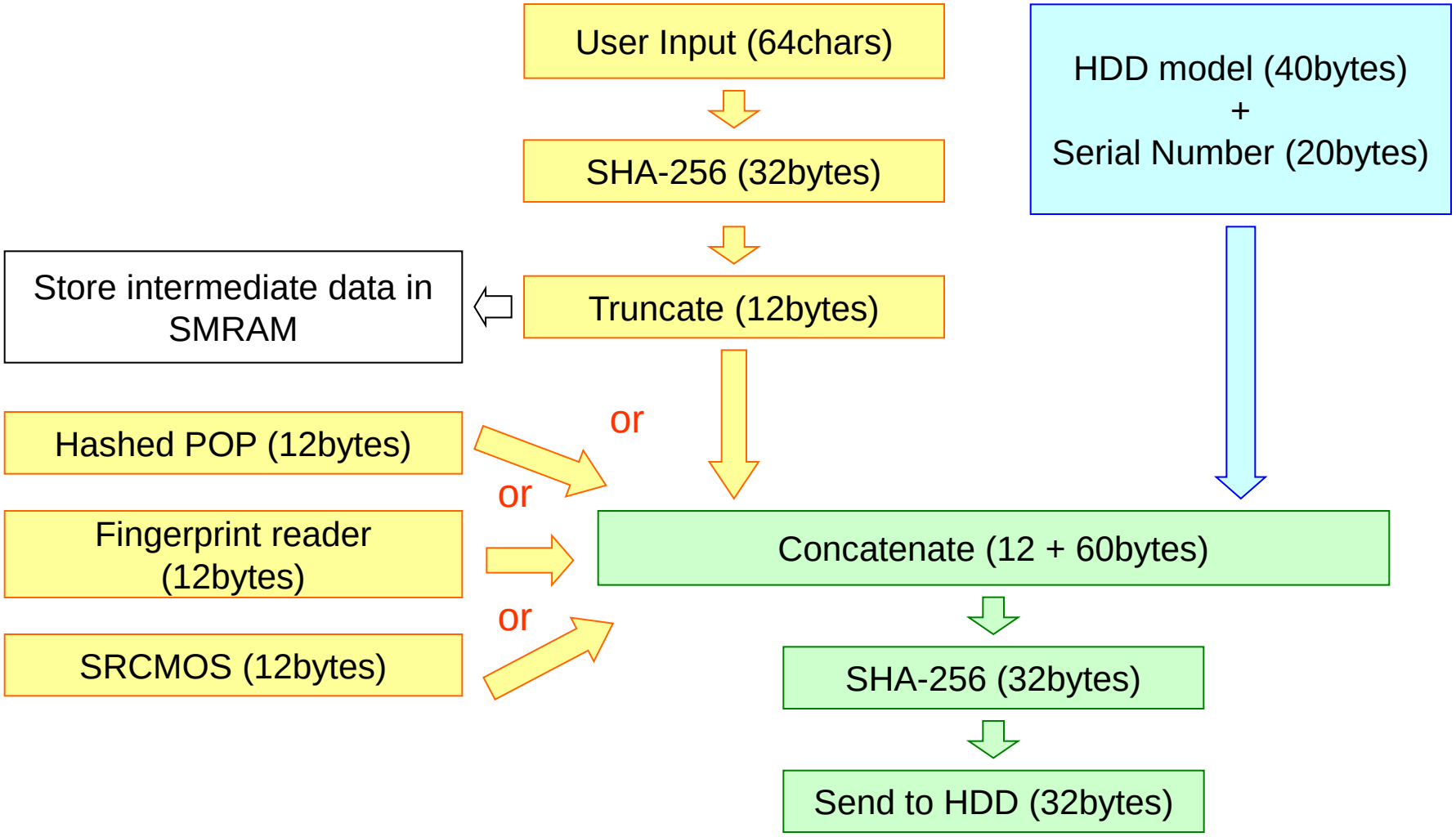
Hard Drive Password

- Requested to input at:
  - Boot
  - Waking up from Hibernate
  - (Not requested at resuming from S3 even if a new HDD is attached or tamper is detected)
- Storage
  - Inside HDD
  - Security feature is locked by SET FREEZELOCK command
    - before exiting POST
    - when the _GTF is evaluated by a storage driver at resuming from S3
- Salting
  - Salted with the hashed Model number and the serial number before sending to HDDs
- Master HDP and User HDP are supported

  [User Only] mode
  - Only User HDP is installed

  [User+Master] mode
  - User HDP and Master HDP are installed
- Old password format (non-32byte format) is not supported

Hard Drive Password generation flow



Master Password Revision Code

- Master Password Revision Code is used to indicate the password format

Utilize of Master Password Revision Code to identify the password format

- **Master Password Revision Code validation (bit 15-14)**
  - 00b : bit 13-0 are invalid. Assume the current format as "Legacy format"
  - 01b : bit 13-0 are valid
  - 10b : Reserved
  - 11b : bit 13-0 are invalid. Assume the current format as "Legacy format"
- **Auxiliary information associated with the Programming Method (bit 13-8)**
- **Programming Method (bit 7-0)**
  - 00h – Legacy format
    - Scan Code or Passphrase
      - bit 13-8 : Reserved 0
      - bit 15-14: 01b
  - 01h – 32byte format
    - 32bytes binary generated by the SHA-256
      - bit 13-8 : Reserved 0
      - bit 15-14: 01b

Unlocking Hard Drive Password

- Identify the HDP format by the Master Password Revision Code
  (IDENTIFY DEVICE information word 92h)

[User Only mode]

- Send the SECURITY UNLOCK command as a user password

(Revision code indicates 32 byte format)

- Send in the 32bytes format
- Three chances

(Revision code indicates legacy format)

- Send both in the 12bytes scan code format and in the 7bytes hash format
- Two chances

[User + Master mode]

- Send the SECURITY UNLOCK command as a user or a master password according to the password prompt mode

(Revision code indicates 32 byte format)

- Send in the 32bytes format
- Three chances

(Revision code indicates legacy format)

- Send both in the 12bytes scan code format and in the 7bytes hash format
- Two chances

Unlocking HDP by POP

- POP is used to unlock a HDD as the User HDP at boot

- POP is NOT used:
  - as the Master HDP
  - when a HDD is attached during S0 and S3

    (Preventing malicious persons from snooping a password by attaching an ATA bus analyzer)

HDD Tamper Detection

- If a HDD is once detached and attached during S3, systems shut down or resume without unlocking in order to prevent malicious person from snooping a HDP by attaching an ATA bus analyzer

[Tamper detection of the primary HDD or mSata HDD]

- Systems shutdown at resuming if the tamper is detected
- Tamper evidence is kept in the EC interface space or PCH GPIO
- Clear the evidence bit before shutdown

[Tamper detection of the Bay HDD]

- Systems resume without unlocking a HDP
- Tamper evidence is kept in the EC interface space
- Clear the evidence bit before resuming

Hot / Warm attach of Hard Drive

- Hot attach (S0)
  - A system must be once enter S4 to unlock a HDP. The HDP is unlocked at waking up from S4.
- Warm attach (S3)
  - A system must be once resume from S3 then enter S4 to unlock a HDP. The HDP is unlocked at waking up from S4.
- Warm attach (S4)
  - A HDP is unlocked at waking up from S4.

e-SATA HDD support

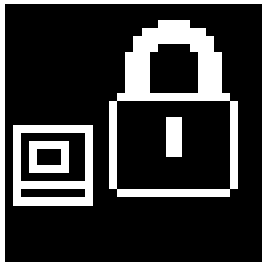
- HDP of the e-SATA HDD is not supported

Password Prompt

Password Prompt behavior

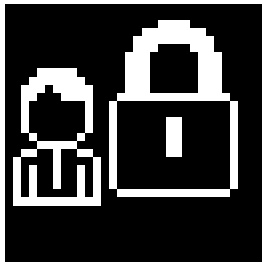
- Acceptable Keys
  - Alphabet (Case insensitive)
  - Number (Numpad is not supported)
  - Space ‘ ‘
  - ‘;’ (To support keyboards that an alphabet is assigned to ‘;’ key of English keyboard)
- Control Keys
  - [Enter] to commit input password
  - [Backspace] to delete one previous input
- Maximum length
  - 64 characters
  - Beep sounds when 65th character is input
- Exceeding retry count
  - Systems show the error icon after three (or two) invalid trials then shutdown automatically.
- Sound feedback (Password Beep) – Supported after GA
- Systems shutdown automatically if no key input in 1minute

Power-On Password Prompt



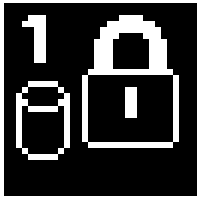
- Either the Power-On Password or the Supervisor Password is accepted
- Displayed when users are requested to input the Power-On Password
- Three chances
- If only the Supervisor Password is installed, pressing [Enter] without any character is accepted. In case, it is assumed that users input valid Power-On Password.
- Power-On Password is requested before Hard Drive Password in order to enable HDP auto unlocking by POP. Whereas, Supervisor Password is requested either before or after Hard Drive Password because of no relationship between them. The request order depends on the events to determine whether Supervisor Password must be requested or not.

Supervisor Password Prompt



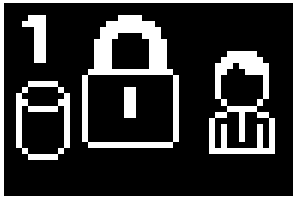
- Only the Supervisor Password is accepted. Power-On Password is NOT accepted
- Displayed when users are requested to input the Supervisor Password
- Three chances

Hard Drive Password Prompt



[User HDP Prompt]

- Only the User HDP is accepted



[Master HDP Prompt]

- Only the Master HDP is accepted
- Available in the User + Master mode only
- Toggled with the User HDP Prompt by the [F1] key

- Displayed when users are requested to input the Hard Drive Password
- Three chances

Password Prompt at Unattended Boot

- Selectable whether the passwords are requested or not when systems boot up by an unattended reason such as WOL, RTC and so on in the BIOS Setup

BIOS password at unattended boot

Enabled (Default):

- Password prompt is displayed
- If there is no key input in 1minute, systems shutdown automatically

Disabled:

- No password prompt is displayed
- BIOS transfers control to OS without any user authentication
- HDPs are unlocked by a POP. If they can not be unlocked, systems shutdown

- The setting is protected by the SVP

Password Prompt at Unattended Boot

Boot reason	Original power State	BIOS Setup 'BIOS password at unattended boot'	Password	If HDP == POP	If HDP <> POP
WOL RI RTC	S4 / S5 (Hibernate/Off) (*1)	Disabled	Not requested	Shutdown or Unlocked by POP automatically(*2)	Shutdown(*4)
		Enabled (Default)	Requested	Unlocked by POP automatically(*3)	HDP is requested

(*1). No difference between S4 and S5.
(*2). Shutdown if AC is not supplied because non-salted POP is not available. BIOS unlocks HDPs by a POP automatically even if users don't input any password. There is a potential risk for HDPs to be snooped. But it's a user's choice.
(*3). Only when users input a valid POP, BIOS unlocks HDPs by a POP automatically.
(*4). If HDPs are installed, systems shutdown immediately without password prompts.

Password Prompt at Reboot

- Selectable whether the passwords are requested or not at reboot

  BIOS password at reboot

  Enabled:
  - Passwords are requested just like boot from off state
  - Enable the SSO at reboot

  Disabled (Default)
  - No passwords is requested
  - BIOS transfers control to OS without any user authentication

- The setting is protected by the SVP
- Passwords are requested regardless of the selection if:
  - Rebooted during POST before valid passwords are input
  - Rebooted from BIOS Setup
  - BIOS Setup is invoked
  - EFI Shell is invoked
  - Signature diskette is detected

Password Prompt at resuming from S3

- Password prompt is never displayed at resuming from S3
  - Hard Drive Password is unlocked at boot only

Password Beep (Supported after GA)

- Selectable whether feedback music sounds or not in the BIOS Setup
- Default is ‘Disabled’
- Events to sound:
  - Password prompt
  - Valid password
  - Invalid password
  - Exceeded retry count

Password Prompt	Sound			
Frequency (Hz)	784	587	784	587
Duration (mS)	200	100	200	250

Valid Password	Sound	
Frequency (Hz)	587	880
Duration (mS)	200	400

Invalid Password	Sound
Frequency (Hz)	415
Duration (mS)	400

Exceeded Retry	Sound		
Frequency (Hz)	415	0	294
Duration (mS)	376	24	500

Note: The frequency 0 means no sound.

BIOS Setup

Password Entry

- Acceptable Keys
  - Alphabet (Case insensitive)
  - Number (Numpad is not supported)
  - Space ‘ ‘
  - ‘;’ (To support keyboards that an alphabet is assigned to ‘;’ key of US English keyboard)

- Control Keys
  - [Enter] to commit input characters
  - [Backspace] to delete one previous input
  - [ESC] to cancel operations

- Maximum length
  - 64 characters
  - Beep sounds and a warning message pops up when 65th character is input

- Exceeding retry count
  - Systems halt with an error message after three (or two for HDP) invalid trials

Power-On Password

- Installing a new password
  - Request to input twice
    - New password
    - Confirm password
  - If the Confirm password is different from the New password, operation is aborted with an error message
  - If the BIOS Setup is invoked without inputting the Supervisor Password, installing a new password is not allowed

Power-On Password (Cont.)

- Changing or Deleting a password
  - Request to input three times
    - Current password
    - New password
    - Confirm password
  - If the Current password is not same as either the installed Power-On Password or the Supervisor Password, the operation is aborted with an error message
  - Systems halt with an error message after three invalid input of the Current Password
  - If the Confirm password is different from the New password, operation is aborted with an error message
  - If the New password and the Confirm password are empty, the password is removed
  - If the BIOS Setup is invoked without inputting the Supervisor Password, deleting the password is not allowed

Supervisor Password

- Installing a new password
  - Request to input twice
    - New password
    - Confirm password
  - If the Confirm password is different from the New password, operation is aborted with an error message

Supervisor Password (Cont.)

- Changing or Deleting a password
  - Request to input three times
    - Current password
    - New password
    - Confirm password
  - If the Current password is not same as the installed Supervisor Password, the operation is aborted with an error message
  - Systems halt with an error message after three invalid input of the Current Password
  - If the Confirm password is different from the New password, operation is aborted with an error message
  - If the New password and the Confirm password are empty, the password is removed

Hard Drive Password

- Installing a new password
  - Request to select **[User]** mode or **[User+Master]** mode

[User] mode (Security Level = Maximum)

- Request to input twice
  - New password
  - Confirm password

[User+Master] mode (Security Level = High)

- Request to input four times
  - New password for the User Hard Drive Password
  - Confirm password for the User Hard Drive Password
  - New password for the Master Hard Drive Password
  - Confirm password for the Master Hard Drive Password

- If the Confirm password is different from the New password, operation is aborted with an error message
- In case of the [User] mode, the input password is also installed as the Master Hard Drive Password
- The Master Password Revision Code is updated to indicate the 32byte format

Hard Drive Password (Cont.)

- Changing or Deleting a password (User mode)
  - Request to input three times
    - Current password
    - New password
    - Confirm password
  - If the Current password is not same as the installed User Hard Drive Password, the operation is aborted with an error message
  - Systems halt with an error message after three or two invalid input of the Current Password
  - If the Confirm password is different from the New password, operation is aborted with an error message
  - If the New password and the Confirm password are empty, the User Hard Drive Password is disabled, the Master Hard Drive Password is set to all null and the Master Password Revision Code is changed to the default value (FFFEh)

Hard Drive Password (Cont.)

- Changing or Deleting a password (User+Master mode)
  - Request to select either **[User HDP]** or **[Master HDP]**
  - Request to input three times
    - Current password
    - New password
    - Confirm password

In case of the [User HDP]

- If the Current password is not same as either the installed User Hard Drive Password or the Master Hard Drive Password, the operation is aborted with an error message
- Systems halt with an error message after three or two invalid input of the Current Password
- If the Confirm password is different from the New password, the operation is aborted with an error message
- If the New password and the Confirm password are empty, the operation is aborted. Removing the User Hard Drive Password is not allowed

Hard Drive Password (Cont.)

In case of the [Master HDP]

- If the Current password is not same as the installed Master Hard Drive Password, the operation is aborted with an error message
- Systems halt with an error message after three or two invalid input of the Current Password
- If the Confirm password is different from the New password, the operation is aborted with an error message
- If the New password and the Confirm password are empty, the User Hard Drive Password is disabled, the Master Hard Drive Password is set to all null and the Master Password Revision Code is changed to the default value (FFFEh)

Protecting BIOS Settings

- Inhibit changing all BIOS settings without inputting the Supervisor Password

Lock BIOS Settings

[Enabled]
All BIOS setting items are grayed out and can't be selected unless the Supervisor Password is input

[Disabled] (Default)
Some of BIOS settings not related to security can be changed without inputting the Supervisor Password

Force minimum length of the passwords

- Force the minimum length of the password
  - The minimum length is checked when a new password is installed or an installed password is about to be changed
  - The setting is not applicable to already installed password
  - Applied to the Power-On Password, the User Hard Drive Password and the Master Hard Drive Password (Not applied to the Supervisor Password)

Set Minimum Length

[Disabled] (Default)
Minimum length is not defined

[4 characters] to [12 characters]
Password length is restricted to equal or longer than selected characters

FDE drive support (Supported after GA)

- Resetting the Cryptographic Key of the FDE drive
  - Resetting the key used for encryption of the data stored in the FDE HDD in order to invalidate all data in a split second
  - The ERASE UNIT command with Enhanced mode resets the key and disables the User Hard Drive Password
  - The Master Hard Drive Password is set to all 0 by the following SET PASSWORD command

Reset the key of the HDD in the HDD bay (or Ultrabay)

- The item is hidden by default and a tool is required to enable it
- The item is available only when a FDE drive is attached

SSD support (Supported after GA)

- Erasing all data stored in SSD
  - Erasing all data stored in the SSD in short period
  - The ERASE UNIT command with Normal mode deletes all data and disables the User Hard Drive Password
  - The Master Hard Drive Password is set to all 0 by the following SET PASSWORD command

Erase contents of the SSD in the HDD bay (or Ultrabay)

- The item is hidden by default and a tool is required to enable it
- The item is available only when a SSD is attached

Credential provider

Releasing password

- If a user is authenticated by a credential provider, the credential provider releases password stored in the corresponding device

- If a released password is invalid or no password is released, the invalid icon is displayed and users are requested to input a password.

Fingerprint Preboot Authentication

- Passwords are stored in the fingerprint reader and retrieved if a finger is authenticated
- Stored password data is NOT salted

[POP]

  - Store the 12 bytes hashed passphrase

[SVP]

  - Store the 7 bytes hashed passphrase

[HDP]

  - Store the 12 bytes hashed passphrase

Hardware Password Manager

- Passwords are stored in the System Vault and retrieved if a user is authenticated with a vault account
- Stored password data is NOT salted

[POP]

- Store the salted 12 bytes hashed passphrase

[SVP]

- Store the salted 7 bytes hashed passphrase

[HDP]

- Store the 12 bytes hashed passphrase (Not salted)

Smart Card Preboot Authentication

- Not supported

Security SMI services

SMI Service - Password Capability and Settings

- Informing Password capability
  - Password format and capability are indicated in the bitmap

```
lnvSecurityPasswordCapability (Sub function = 82h)
  (On Entry)
    None

  (On Exit)
    EBX - Password capability
            Bit 0 : Support Password update    (Always 1)
            Bit 1 : Support Long Password      (Always 0)
            Bit 2 : Support Passphrase         (Always 1)
            Bit 3 : Passphrase mode            (Always 1)
            Bit 4 : SVP installation           (1=Installed)
            Bit 5 : Support 32byte HDP         (Always 1)
```

SMI Service - Password Hashing

- Generating a SHA-256 hash of a password
  - Calculating a SHA-256 hash of a password
  - Salting is not applied
  - Hashed password is returned after 8 continuous calls

lnvSecuritySHA256Passphrase (Sub function = 90h)

```
(On Entry)
  EBX – Character offset 00 - 03h
  ECX – Character offset 04 – 07h
  ESI – Index

(On Exit)
  EBX – Hash offset 00 – 03h (when index = 7)
  ECX – Hash offset 04 – 07h (when index = 7)
  EDI – Hash offset 08 - 0Bh (when index = 7)
  ESI – Next index
```

SMI Service - Power-On Password Validation

- Validating a Power-On Password
  - Return if the password is valid or not
  - Password is passed though the registers in the hashed format generated by the Password Hashing SMI Service (Not Salted)
  - After three invalid trials, the service is frozen and never validates the password until systems reboot

lnvSecurityCheckPop (Sub function = 11h)

```
(On Entry)
  EBX – POP offset 00 - 03h
  ECX – POP offset 04 – 07h
  ESI – POP offset 08 – 0Bh

(On Exit)
  EAX – bit22      : 0 = Valid
                   : 1 = Invalid
  EAX – bit23      : 0 = Retry count is not exceeded
                   : 1 = Retry count is exceeded
```

SMI Service – Supervisor Password Validation

- Validating a Supervisor Password
  - Return if the password is valid or not
  - Password is passed though the registers in the hashed format generated by the Password Hashing SMI Service (Not Salted)
  - After three invalid trials, the service is frozen and never validates the password until systems reboot

```
lnvSecurityCheckPap (Sub function = 5h or A0h)
  (On Entry)
    EBX – SVP offset 00 - 03h
    ECX – SVP offset 04 – 07h (07h is only for sub function A0h)
    ESI – SVP offset 08 – 0Bh (Only for sub function A0h)

  (On Exit)
    EAX – bit22      : 0 = Valid
                     : 1 = Invalid
    EAX – bit23      : 0 = Retry count is not exceeded
                     : 1 = Retry count is exceeded
```

SMBIOS

SMBIOS – Password Status

- Hardware Security (Type 24)
  - Indicate installation status of the Power-On Password and the Supervisor Password

Offset	Name	Length	Value	Description
00h	Type	BYTE	24	Hardware Security indicator
01h	Length	BYTE	05h	Length of the structure.
02h	Handle	WORD	Varies	The handle, or instance number, associated with the structure.
04h	Hardware Security Settings	BYTE	Bit-field	Identifies the password and reset status for the system: Bits 7:6 *Power-on Password Status*, one of: 00b Disabled 01b Enabled 10b Not Implemented 11b Unknown Bits 5:4 *Keyboard Password Status*, one of: 00b Disabled 01b Enabled 10b Not Implemented 11b Unknown Bits 3:2 *Administrator Password Status*, one of: 00b Disabled 01b Enabled 10b Not Implemented 11b Unknown Bits 1:0 *Front Panel Reset Status*, one of: 00b Disabled 01b Enabled 10b Not Implemented 11b Unknown

SMBIOS – Password Status

- Hard Drive Password Security Status (Type 132)
  - Indicate installation status of the Hard Drive Password

Offset	Name	Content	Example
00h	Type	84h (132)	
01h	Length	07h	
02h	Handle		
04h	Revision	01h for the following format	01h
05h	HDP Security Status	Bits 14:12 HDP Security Status for HDD5 Bits 11:9 HDP Security Status for HDD4 Bits 8:6 HDP Security Status for HDD3 Bits 5:3 HDP Security Status for HDD2 Bits 2:0 HDP Security Status for HDD1 Each bit is: 000b: Disabled 001b: High 010b: Maximum 011b: Not attached	0000000000000010b

thank you grazie **merci** danke **grazias** 謝謝 спасибо
gracias **obrigado** ありがとう **dank** takk **bedankt** dakujem

lenovo
NEW WORLD. NEW THINKING.