DELL Technologies

Enhanced User Credential Protection with Dell SafeID

December 2024

User credentials are the keys to an organization’s data kingdom

The theft of user credentials has become more common due to:

Digital Transformation: As more services move online, user credentials become a gateway to a range of platforms. Attackers recognize this and focus on stealing them.

Remote Work: The rise of remote work has increased reliance on digital tools. Attackers exploit this shift by targeting remote workers and their home networks, which are often less protected than corporate networks.

Automation: Automated tools allow attackers to test large sets of credentials quickly. They can launch attacks at scale, increasing the chances of success.

Supporting facts:

Cyberattacks using valid user credentials spiked by 71% in 2023.

These attacks involve malicious actors gaining access to systems by using legitimate login information [1].

Abuse of legitimate credentials constituted a third of all cyberattacks on enterprises.

In other words, attackers are increasingly exploiting existing user accounts to infiltrate organizations [1]. Attackers recognize that having access to valid account credentials reduces the need for extensive phishing campaigns[2].

Organizations often overlook basic security practices.

Misconfigurations in web applications, such as allowing concurrent user sessions, weaken **multi-factor authentication (MFA)**. These vulnerabilities create opportunities for identity-based attacks. **30% of all application vulnerabilities** stem from security misconfigurations[2].

1. https://techmonitor.ai/technology/cybersecurity/valid-user-credentials-ibm
2. Hackers using stolen credentials to launch attacks as info-stealing peaks | CSO Online

Copyright © Dell Inc. All Rights Reserved.

Dell SafeID – An innovative way to secure user credentials

Dell SafeID isolates identity-related operations and data from the operating system environment and memory and protects them in hardware, making them far less vulnerable to attack and exfiltration.

All processing and storage of user authentication data takes place within a dedicated chip. For PCs with fingerprint and smart card readers, SafeID also includes a unique hardware-based security solution - a hardened and secure “bank” known as ControlVault-which stores and processes user biometric templates and security codes in FIPS-certified hardware.

Dell SafeID always includes Trusted Platform Module (TPM) security technology built into its computer system boards. TPM provides enhanced security against vulnerabilities by using cryptography to protect critical information on PCs and enable platform authentication. Dell TPM's are FIPS 140-2 (and in one case FIPS 140-3) validated and TCG Certified (with Common Criteria Certification analogous to Smart Cards and Payment Cards).

Copyright © Dell Inc. All Rights Reserved.

Dell SafeID goes beyond the OS to secure user credentials

Hardens end-user credentials

Stores and executes code using a secure processor

Stores end-user credentials to allow a single point of migration

Supports a broad set of crypto algorithms

Secures & Isolates Encryption Keys and Templates

SafeID executes operations and stores credentials within its secure boundary which allows credentials to be kept secure and protected against any inspection or modification of the execution process.

SafeID stores the execution code for secure processes within this secure boundary keeping malicious applications from accessing it.

Seals Off Code Execution & Storage

Dell SafeID lets applications store keys and templates within a protected boundary that is strictly controlled.

All usage of keys and templates are isolated from the host so they are never exposed to attacks.

Copyright © Dell Inc. All Rights Reserved.

Understanding the lines of SafeID defense in a Dell Commercial PC

Dell TPM

- The TPM improves the security of all Dell PCs by creating and protecting encryption keys and enabling platform attestation
- TPM has been in use for over 20 years and has been part of PCs since around 2005.
- The TPM is a secure crypto-processor attached to a device to establish secure operations. TPM helps to protect a device and its sensitive data by storing the relevant keys vital for encryption, decryption and authentication.

Dell ControlVault

- Dell ControlVault is designed for uniquely securing user credentials in a Dell device
- It is an added security solution from Dell to provide an additional layer of security to users' credentials.
- It is a hardware-based security solution that provides a secure bank that stores passwords, biometric templates, and security codes within the hardware. It enables and secures Fingerprint, Smartcards, and Near-field communications (NFC).

Both Dell TPM and Dell ControlVault are dedicated hardware chips. How does ControlVault differ from TPM?

ControlVault stores user credentials while TPM stores encryption keys. TPM has Common Criteria certification, while ControlVault does not.

Dell TPM 2.0 has a very rich authorization system now and is cryptographically agile, supporting SHA-256, SHA-384 and soon to be SHA-512, which provides 32, 48, and 64B (meaning 256 bits, 384 bits and 512 bits).

Other secure mechanisms in your Dell device to protect user identity:

Fingerprint scanners on Dell devices also come with Match-on-chip technology (MoC). MoC is fingerprint reader technology that stores biometric credentials on a separate chip. MoC systems offer higher security than Match-on-Host systems because they store the user's biometric data on a separate MCU.

Copyright © Dell Inc. All Rights Reserved.

Dell ControlVault amplifies security for Dell SafeID

Dell ControlVault – a part of Dell SafeID for PCs with fingerprint readers and smart cards - is a hardware-based security solution that provides a secure bank which stores your passwords, biometric templates, and security codes within the firmware.

Third-party verification

ControlVault meets the benchmark for validating the effectiveness of cryptographic hardware.

Latest and greatest

The current version of Dell ControlVault comes with improved specs like Double Storage Capacity, Secure Boot ROM enhancements and upgraded functionalities to ensure it continues to meet excellence in securing user credentials.

Dell ControlVault's uniqueness lies in its ability to isolate security operations

Dell ControlVault helps protect secure operations by isolating them from the Windows® environment and memory. Instead, all processing and storage of critical data takes place in a dedicated chip providing isolated process and memory — providing a protective and secure boundary. This isolation removes the processing and storage of identity and biometric information from unsecured operating systems and physical hard drives.

Copyright © Dell Inc. All Rights Reserved.

Dell ControlVault Technical Data

Public Key Accelerators (PKAs) enhance cryptographic efficiency and security by offloading intensive tasks like key exchanges, signatures, and encryption/decryption to specialized hardware, ensuring secure key handling with minimal performance impact.

PKA (Public Key Accelerator)

Public Key Acceleration

- Diffie-Hellman public value and shared key computation of modulus up to 4096 bits
- 2048-bit DSA signature with SHA-256 hash
- RSA encryption with key sizes up to 4096-bit key size
- RSA decryption with key sizes up to 4096-bits (Chinese Remainder Theorem)
- RSA key generation with Rabin-Miller number selection
- Elliptic curve Diffie-Hellman in prime field GF(p)
- Prime field EC-DSA signature for modulus sizes up to 521 -bit
  - ECDSA-p256, ECDSA-p384, ECDSA-p521 prime field ECC point operations
- Generic prime field ECC point operations
- Generic long integer math operations
- NIST prime field ECC curve optimization

SMAU Bulk Data Crypto – Primitive Cryptography Algorithms Supported

Primitive Crypto Algorithms	Algorithms Properties	Crypto Algorithm Key Lengths or Output Lengths	Cryptography Protocol/Standard	Function
AES-ECB	AES, Symmetric, ECB (Electronic CodeBook) mode	128/192/256-bit key	FIPS 197	Confidentiality (Encryption/Decryption)
AES-CBC	AES, Symmetric, CBC (Ciphyer Block Chaining) mode	128/192/256-bit key	FIPS 197	Confidentiality (Encryption/Decryption)
AES-CTR	AES, Symmetric, CTR (Counter) mode	128/192/256-bit key	FIPS 197	Confidentiality (Encryption/Decryption)
AES-CCM	AES, Symmetric, CCM (Counter with Cipher-block-chaining Message authentication code) mode	128-bit key	SP 800-38C	Authentication/ Confidentiality
HMAC-SHA256	Symmetric	256-bit MAC	FIPS 198-1	Authentication
SHA-256 or SHA256		256-bit digest	FIPS180-4	Integrity
SHA3-224		224-bit digest	FIPS 202	Integrity
SHA3-256		256-bit digest	FIPS 202	Integrity
SHA3-384		384-bit digest	FIPS 202	Integrity
SHA3-512		512-bit digest	FIPS 202	Integrity

Dell ControlVault Advantage: Most applications store encryption keys on the hard drive, posing a security risk as hackers can find them despite obfuscation. ControlVault, however, stores keys within a protected boundary with strict access controls. Only authorized applications, as defined by the owner or IT manager, can access these keys. Additionally, Dell ControlVault has a small memory footprint, ensuring minimal impact on system performance.

Copyright © Dell Inc. All Rights Reserved.

Updated Dell ControlVault

New and improved

Updated Specs

- **Double Storage Capacity (1MB – 2MB)** : The latest ControlVault 3 specification boasts an impressive storage capacity, doubling from 1MB to 2MB. More storage translates to the ability to capture up to 10 fingerprint images, allowing for robust biometric data collection. This not only reduces risk but also minimizes false positive readings.
- **Double secure key storage space:** More storage and stronger keys that binds to the host. This was one of the reasons what kept Dell commercial devices safe during some recent vulnerabilities.
- **Secure Boot ROM enhancements:** ControlVault is equipped with settings stored in ROM during the manufacturing process. Additionally, the Random Number Generator (RNG) is employed to generate cryptographic keys. This dual-layer approach enhances security and serves to protect the system's initial memory.
- **A new TRNG (true Random Number Generator) SP 800-90B ESV certified**: True RNGs add to reducing risk in the generation of credential keys.

Improved features

- **FIPS 201 Full Scan Fingerprint Reader and ControlVault with Roaming Credentials**: Dell ControlVault works with leading biometric matching solutions for health care and other industries. This means we will have ability to provide roaming credentials solutions like Imprivata and Digital Persona.
- **Fingerprint Self-Learning Support w/ControlVault 3+:** Enhances user recognition and security by adapting to your unique fingerprint. The more you use the fingerprint reader, the better it performs, resulting in fewer false positives and a reduction in risk. It's another way Dell prioritizes seamless user experiences and robust security.
- **Dell eDiags support launching on CV3+ with Delta II:** ControlVault 3+ has the ability to run diagnostics to enable testing and validation before deployment, ensuring your credentials are safe from the beginning.

Copyright © Dell Inc. All Rights Reserved.

SafeID with TPM strengthens user credential security

The Trusted Platform Module (TPM) is a chip that resides inside a computer and is soldered to the system board on Dell computers. A TPM's primary function is to securely generate cryptographic keys, but it has other functions as well. Each TPM chip has a unique and secret RSA key that is embedded into it on production. Watch this video to learn about Trusted Platform Module on Dell.

About TPM

Here's how TPM works:

When a device is powered up, TPM authenticates it by providing a cryptographic key to unlock the encrypted drive. If the key is valid, the computer will boot up normally. If the key is tampered with, the computer won't start.

Where is TPM used?

TPM 2.0 is an essential tool for security within operating systems such as Windows 11. Through the TPM 2.0, important features such as Windows Hello for identity protection and BitLocker for data protection can be utilized, making it an indispensable component of a device's security.

TPM is used for multiple features that increase the security of your Dell device.

BitLocker Drive Encryption: Automatically encrypts the system drive to keep your data safe.

Device Attestation: Microsoft uses the TPM for Device Health Attestation, and Dell SCV uses it to attest to the hardware configuration of the platform.

Windows Hello: Secure user authentication without a password.

Secure Boot and Measured Boot: Block malicious drivers and rootkits from intercepting the boot process of the operating system.

Trusted Platform Modules (TPMs) are certified by the following:

- **Common Criteria (CC)** certified EAL4+ augmented with ALC_FLR.1 and AVA_VAN.5
- **FIPS 140-2 Level 2** certified with physical security level 3
- **Trusted Computing Group** (TCG) certified

Copyright © Dell Inc. All Rights Reserved.

Discrete TPM benefits your devices in multiple ways

Authenticate devices / platforms

When a device is powered up, the TPM authenticates it by providing a cryptographic key to unlock the encrypted drive.

Secure against threat

TPMs can help provide security against threats like firmware and ransomware attacks. They can also add an extra layer of protection so potential malware cannot access sensitive user data.

Monitor and report on the computer's configuration

The TPM maintains a secure record of measurements provided to it by the platform firmware and OS.

Generate Attestation Keys (AK)

TPMs creates and protects Attestation Keys (AK), which can be cryptographically bound to Endorsement Key (EK), which provides privacy and anonymity when communicating with different parties.

Additional layer of security for Dell devices with Dell Technologies Supply Chain Security

A core element of Dell’s security-enabled supply chain program is **Secured Component Verification (SCV)**, now available on Dell Commercial PCs as well as the Dell PowerEdge portfolio.

SCV enables IT administrators to validate the componentry of incoming systems to ensure that the configuration is identical to what has been manufactured and secured by the TPM. It also ensures that components and configurations set at time of manufacture conform to the specifications set by the customer, and remain so throughout the journey, from factory to customer.

Any component changes that occur after a device leaves the Dell factory, and before the verification is run, will show up as a mismatch in the resulting report. This allows customers to account for authorized changes and to identify unauthorized changes.

Copyright © Dell Inc. All Rights Reserved.

About Dell Endpoint Security

Dell SafeID is part of the larger Dell Trusted Workspace endpoint security portfolio. Through Dell Trusted Workspace, customers can access “built-in” and ”built-with” security features, as well as “built-on” software-based protections, to help ensure a comprehensive defense framework for today’s evolving threat landscape.

Built-in & Built-with Security

Hardware & firmware protections for Dell commercial PCs

Dell SafeBIOS: Mitigate the risk of BIOS and firmware tampering though Dell’s exclusive[1] off-host BIOS verification, BIOS Image Capture and BIOS Events and Indicators of Attack.

Dell SafeID[2] : Only Dell[1] secures end user credentials in a dedicated security chip, keeping them hidden from malware that looks for and steals credentials.

Dell SafeSupply Chain[3] : Gain assurance that PCs are safe from the first boot with supply chain security solutions, such as Secured Component Verification, tamper-evident packaging and NIST-level hard drive wipes.

Built-on Security

Software protections for Dell and non-Dell devices alike

Dell SafeGuard and Response (powered by CrowdStrike and Secureworks): Prevent, detect, and respond to advanced malware and cyber-attacks to stay productive and free from the disruption and churn an attack can cause.

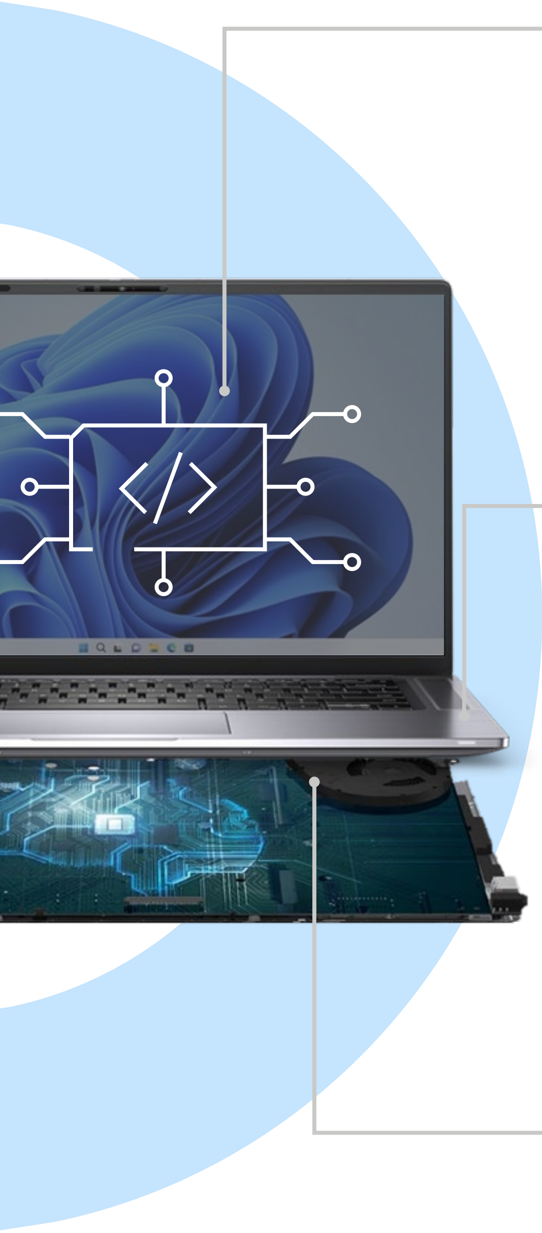
Dell SafeData (powered by Absolute and Netskope): Protect sensitive data on device to help meet compliance regulations, and secure information in the cloud giving end users the freedom to safely collaborate.

1 Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. https://www.principledtechnologies.com/Dell/OEM-security-feature-comparison-0424.pdf, April 2024. 2. Features vary by model. 3 Availability may vary by product, region and market.

Copyright © Dell Inc. All Rights Reserved.

Dell Trusted Workspace

Multiple layers of defense



Built-on
Software Security

Layer on advanced threat protection with software from an expertly selected partner ecosystem. Take advantage of the benefits and efficiencies that come from consolidating security purchases.

Built-in
Hardware & Firmware Security

Prevent and detect foundational attacks with the world's most secure commercial AI PCs.[1] Deep defenses at the BIOS/firmware and hardware levels keep the device protected in-use.

Built-with
Supply Chain Security

Work confidently knowing your device is secure from first boot. Secure PC design, development and testing help reduce the risk of product vulnerabilities. Rigorous supply chain controls reduce the risk of product tampering.

Prevent, detect and respond to threats wherever they occur

Dell SafeGuard and Response

Dell SafeData

Stay protected from evolving threats

Dell SafeBIOS

Dell SafeID

Trust hardware is tamper-free on delivery

Dell SafeSupply Chain

[1] Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies, A comparison of security features, April 2024.

Copyright © Dell Inc. All Rights Reserved.

Learn more

Contact a Dell Endpoint Security Specialist at global.security.sales@dell.com for more information about solutions to help improve your security posture.

Learn more at www.Dell.com/endpoint-security

Additional Resources

- Dell SafeID datasheet
- About Dell ControlVault
- Dell ControlVault Driver and Firmware
- How to enable TPM on your Dell computer
- Activating the Trusted Platform Module Security Feature
- How to Successfully Update the TPM Firmware on your Dell Computer

Copyright © Dell Inc. All Rights Reserved.