The combination of a properly designed password storage method and a properly designed methodology/policy for a user password choice is absolutely critical. Enter TPM, the Trusted Platform Module, created by Trusted Computing Group. TPM is kind of a digital fingerprint, a microcontroller that stores keys, passwords and digital certificates, enabling:  

- **Secure repository for certificates, keys, passwords that’s safer than storing these in software**

**Cryptographic capabilities to create a unique digital fingerprint for systems**

Over two billion TPMs are embedded into PCs, servers, networking gear and other devices, protecting users against unauthorized changes: TPM stores personal data, making it more secure from software attack and physical theft.

**Access to data and secrets in a platform can be denied by policy settings, making critical applications and capabilities such as secure email, secure web access and local protection of data much more secure.**

**TPM 2.0**

- **Increased cryptographic strengths:** TPM 2.0 supports additional cryptographic algorithms, including those defined in the New European Norms (X9.24, X9.25) and algorithms defined by the National Institute of Standards and Technology (NIST). The TPM 2.0 protocol is also updated to support these new algorithms.
- **Enhanced key management:** TPM 2.0 provides a more flexible key management model, allowing for a larger variety of key types and sizes, including support for quantum-resistant algorithms.
- **Improved security features:** TPM 2.0 includes enhancements to the platform’s security features, such as improved support for secure boot and system integrity checking.
- **Integration with other security technologies:** TPM 2.0 is designed to work seamlessly with other security technologies, such as remote attestation and secure boot.

**What is TPM 2.0?**

- **TPM 2.0** is an extension of the Trusted Platform Module (TPM) specification, which provides a set of security primitives that can be used to protect the integrity of a computer system. TPM 2.0 builds upon the capabilities of TPM 1.2 by introducing new features and algorithms.
- **TPM 2.0** was developed by the Trusted Computing Group (TCG) and is currently supported by a wide range of hardware and software vendors.

**Where can I find more information about TPM 2.0?**

- **Development:** The TCG provides detailed information about the TPM 2.0 specification on their website.
- **Implementations:** Many hardware and software vendors have implemented TPM 2.0 in their products, and you can find information about these implementations on their websites.
- **Papers and Whitepapers:** There are many papers and whitepapers available that provide in-depth information about TPM 2.0, including its benefits, implementation, and use cases.