SecureDoc™
by WinMagic

ICMC 2017

Development of cPPs for Full Disk Encryption

Garry McCracken CISSP, VP Technology

WINMAGIC®

Abstract

Software Full Drive Encryption (FDE) -- Formerly known as Full Disk Encryption -- has been the prime choice for protecting the confidentiality of data at rest (DAR) on laptops for over a decade, but more and more Self-Encrypting Drives (SEDs) are becoming the obvious choice for FDE because of their advantages in performance, transparency and security.

The standard assurance approach for software FDE in the past has been FIPS 140-2 and Common Criteria EAL evaluations by third party accredited labs, but there are difficulties with this approach for software FDE, let alone SEDs.

To address these issues, International Technical Community (iTC) work groups were formed to create collaborative Protection Profiles (cPP) for FDE. This presentation provides an introduction to the set of cPPs for Full Drive Encryption (FDE) and explains how they relate to each other.

About WinMagic

Founded

1997

Headquarters

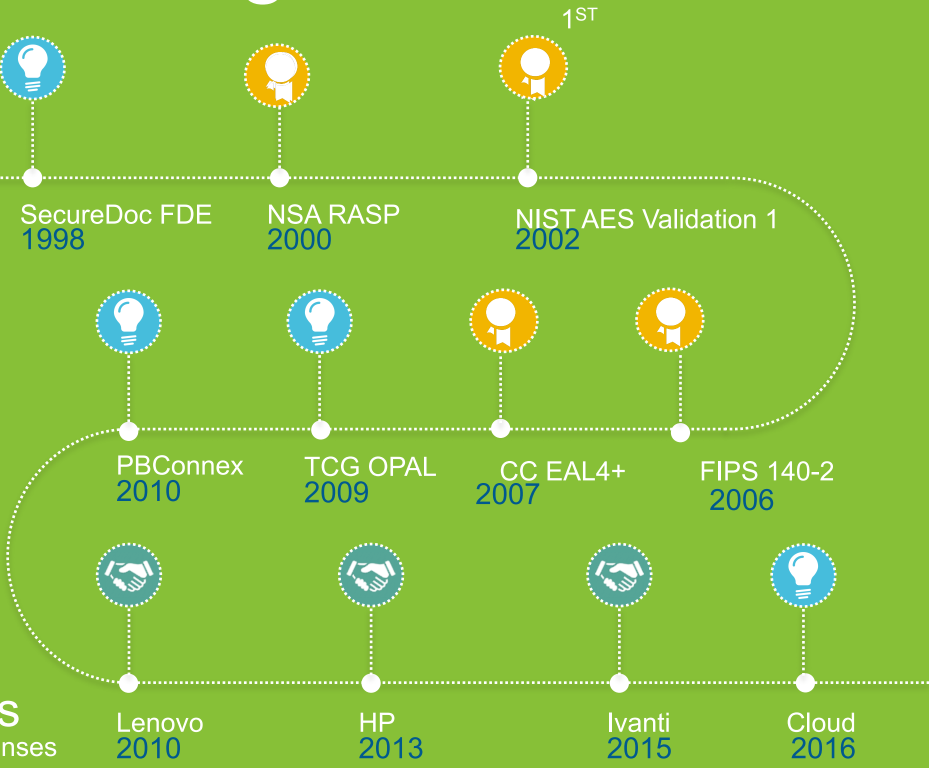
Toronto

Canada

Customers

84 Countries

8+ Million Active Licenses



1^{ST}

SecureDoc FDE
1998

NSA RASP
2000

NIST AES Validation 1
2002

FIPS 140-2
2006

CC EAL4+
2007

TCG OPAL
2009

PBConnex
2010

Lenovo
2010

HP
2013

Ivanti
2015

Cloud
2016

SecureDoc™
Data Security

Architecture for Endpoint Encryption

Two Components to the Ideal FDE Solution.

Key Management

Component (cPP AA +EM)

Authentication
PBConnex + MFA

Intelligent Key Management
SecureDoc Enterprise Server

Identity Management
AD/LDAP Integration + Sync

Encryption

Component (cPP EE)

Hardware-based Crypto
OS-Agnostic Management

Native OS-based Crypto
Next-Level Integration

ISV Software-based Crypto
Leading Full Disk Encryption

Trusted Computing Group
OPAL and Enterprise SEDs

Microsoft
BitLocker

Apple
FileVault 2

WinMagic
SecureDoc FDE

SecureDoc™
by WinMagic

Historical Approach for FDE: CC EAL

- Security Target – EAL (Evaluation Assurance Level)”
- Unique to each product
- Difficult for customers to compare
- Evaluations time consuming
- Evaluations expensive

SecureDoc™ by WinMagic

collaborative Protection Profiles (cPP) for FDE

- Technical Community (iTC) work groups formed with subject matter experts from the
- labs, academia, **industry** and governments
- No EAL level with cPPs
- All the “must have” security functions for FDE
- Practical
- Implementable
- Comparable
- First cPPs for FDE were completed in January 2015

SecureDoc™ by WinMagic

Full Drive Encryption Protection Profiles

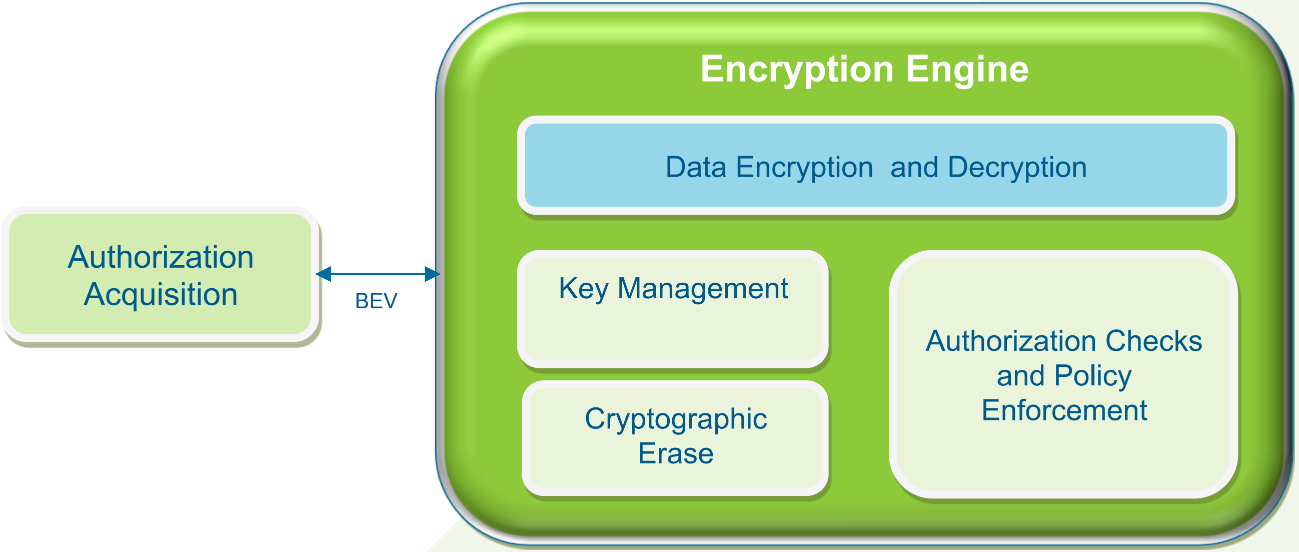
Full Drive Encryption cPPs

- cPP EE - *Encryption Engine* *(V2.0 Sept 2016)*
- cPP AA - *Authorization Acquisition* *(V2.0 Sept 2016)*
- cPP EM - *Enterprise Management* *(in review*)*

- ** The public comment period ends May 26, 2017: https://www.commoncriteriaportal.org/communities/fde.cfm*

SecureDoc™ by WinMagic

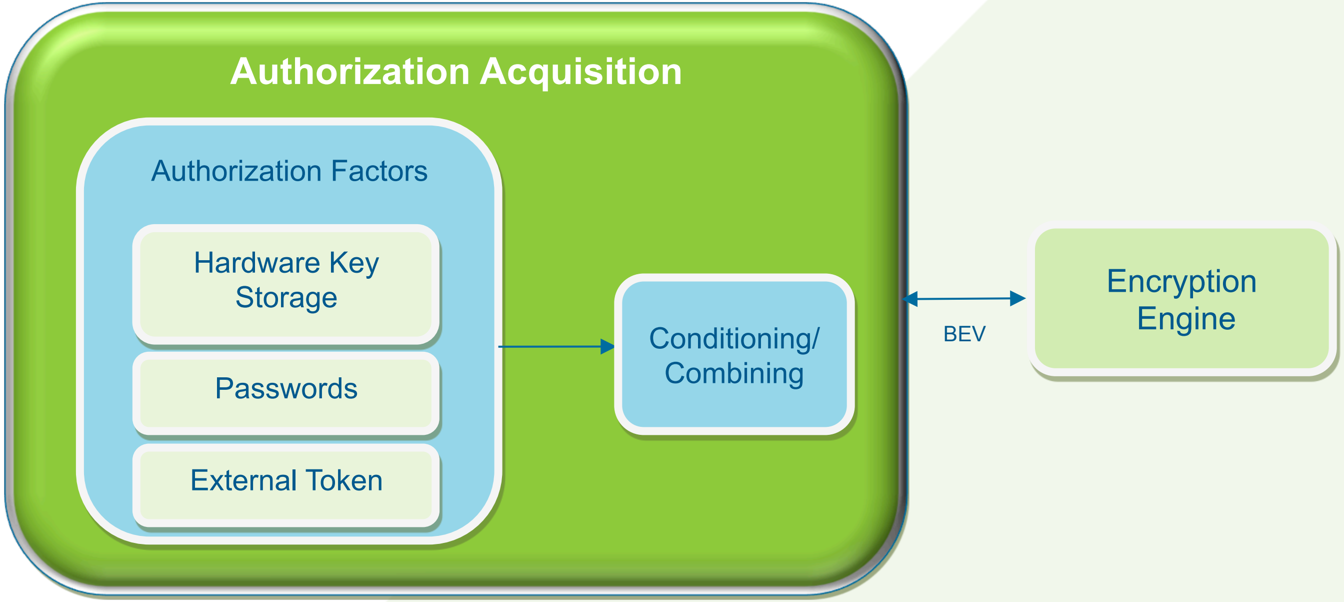
FDE EE cPP – *Encryption Engine*


Encryption Engine
Data Encryption and Decryption
Authorization Acquisition
BEV
Key Management
Cryptographic Erase
Authorization Checks and Policy Enforcement

Describes the requirements for the Encryption Engine piece and details the necessary security requirements and assurance activities for the actual encryption/decryption of the data by the DEK

SecureDoc™ by WinMagic

FDE AA cPP - *Authorization Acquisition*

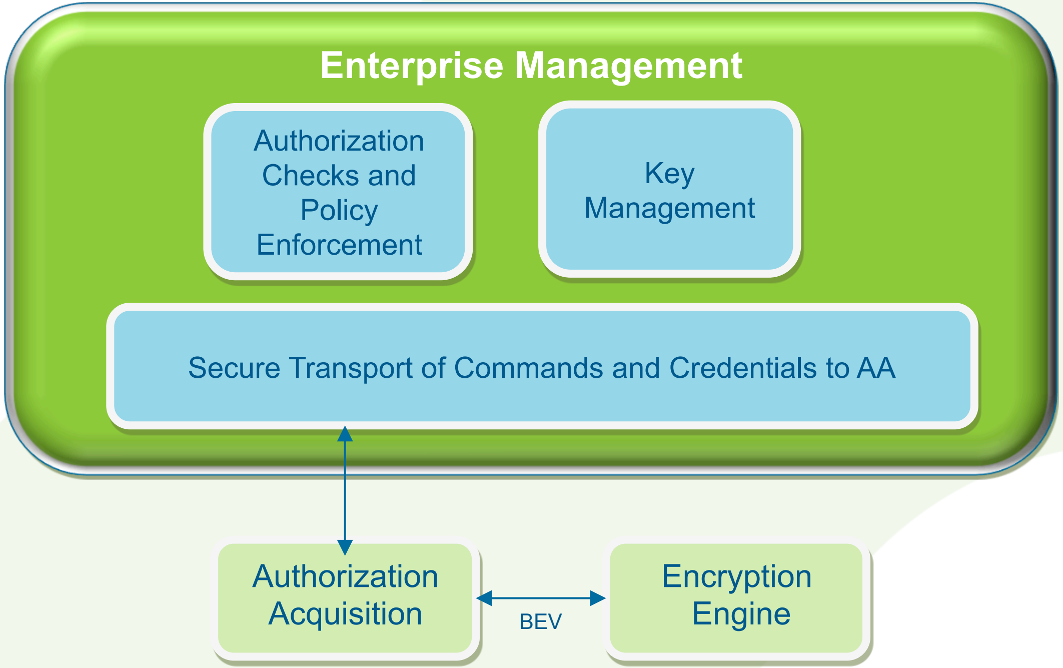


Describes the requirements for the Authorization Acquisition piece and details the security requirements and assurance activities necessary to interact with a user and result in the availability of sending a Border Encryption Value (BEV) to the Encryption Engine

SecureDoc™ by WinMagic

FDE EM cPP – *Enterprise Management*

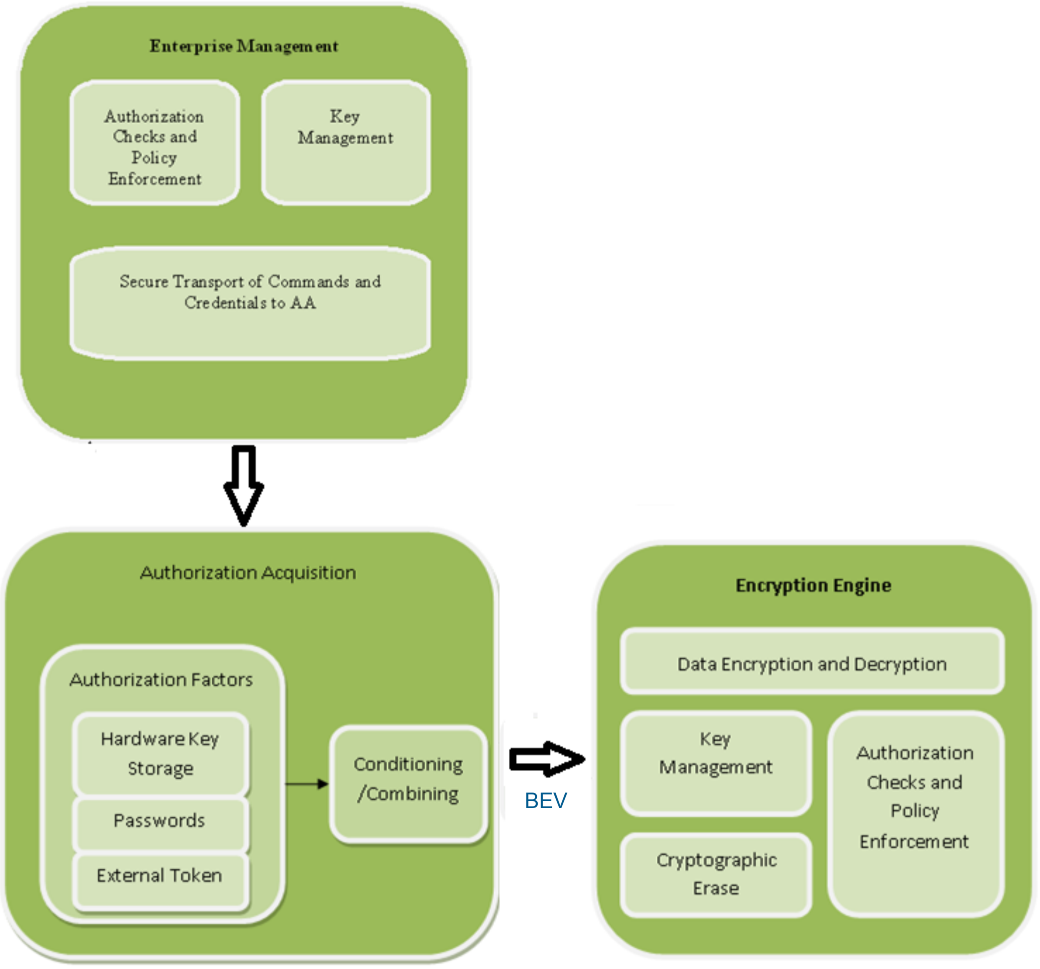
NEW! Describes the requirements for the enterprise management (from a server) of the end point consisting of an AA and EE.



Enterprise Management
Authorization Checks and Policy Enforcement
Key Management
Secure Transport of Commands and Credentials to AA
Authorization Acquisition
BEV
Encryption Engine

FDE cPP Solutions

cPP	Description
(AA + EM)	Host software provides the interface to a self-encrypting drive and Administrative software that allows enterprise management of the interface.
(AA + EM) + EE	A enterprise manageable software full drive encryption solution
AA + EE	A standalone solution without enterprise management (pure software or hybrid)



Enterprise Management

Authorization Checks and Policy Enforcement

Key Management

Secure Transport of Commands and Credentials to AA

Authorization Acquisition

Authorization Factors

Hardware Key Storage

Passwords

External Token

Conditioning /Combining

BEV

Encryption Engine

Data Encryption and Decryption

Key Management

Cryptographic Erase

Authorization Checks and Policy Enforcement

Applications for cPPs

- Who will use them?
- Who will want them?

SecureDoc™ by WinMagic

Self-Encrypting Drive Manufacturers

- Trusted Computing Group - Opal Certification Program
  - Announced April 12, 2016
  - TCG-certified test suite (Test cases)
  - cPP EE (Security Evaluation)

TRUSTED COMPUTING GROUP®

SecureDoc™ by WinMagic

Independent Software Vendor (ISV)

- Standalone
  - cPP AA + cPP EE SED
  - cPP AA + cPP EE SW
- Enterprise Managed
  - cPP AA + cPP EM for cPP EE SEDs and SW encryption

SecureDoc™ by WinMagic

Endorsements

- cPP EE & cPP AA:
  - NIAP (United States)
  - CCCP (Canada)
  - AISEP (Australia & New Zealand)
  - CESG (United Kingdom)
- cPP EM – None (Not published yet)

SecureDoc™ by WinMagic

Thank You!

For further information, please contact

garry.mccracken@winmagic.com

SecureDoc™ by WinMagic