Hewlett Packard Enterprise

HPE プラットフォーム証明書検証ツールのデモ

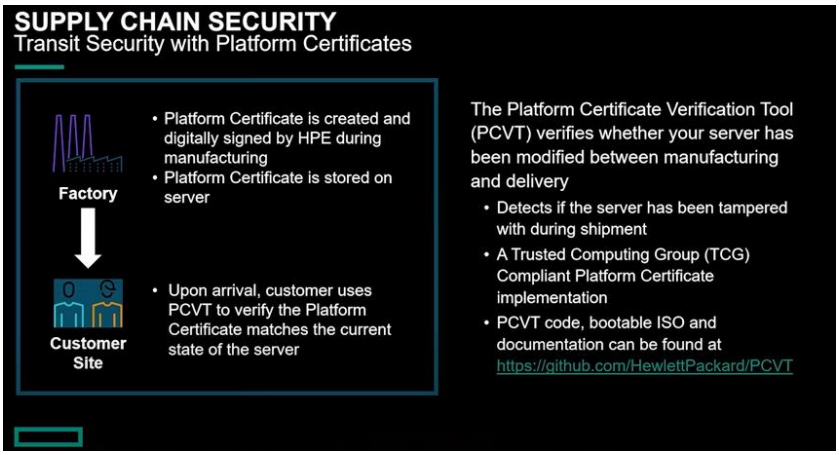
目的

本資料を参照いただくことで、プラットフォーム証明書について内容をわかりやすくご理解いただけます。

本資料には、以下のコンテンツが含まれます。

- プラットフォーム証明書とは何か
- PCVT（プラットフォーム証明書検証ツール）のデモ（改ざんをしていない状態）
- PCVT（プラットフォーム証明書検証ツール）のデモ（改ざんをした状態）
- プラットフォームコンポーネント検証の判定
- 詳細情報の入手

プラットフォーム証明書とは？



プラットフォーム証明書は、お客様のサプライチェーンを保護することを目的として HPE が配備した業界標準の技術です。

お客様のサーバーが HPE の工場で製造され、出荷時の状態からお客様の元へ届くまで改ざんされていないことを証明します。

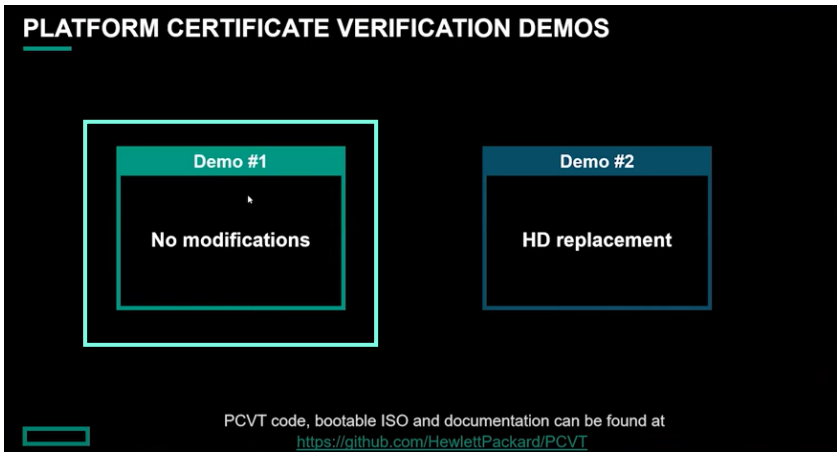
製造の段階で HPE はプラットフォーム証明書を作成し、暗号した署名を行います。

プラットフォーム証明書はサーバー上に保持されているため、サーバーと共に出荷されます。

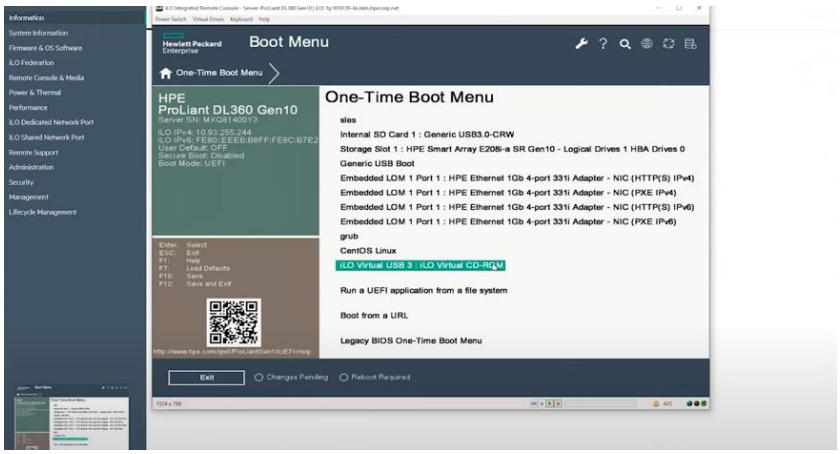
サーバーがお客様のもとに届いた際、お客様はプラットフォーム証明書検証ツール (PCVT) を用いてそのサーバーが工場出荷時から改ざんがされていないかを検証することができます。

プラットフォーム証明書は TCG (Trusted Computing Group) に準拠していることに加え、HPE は更に PCVT というオープンソースツールを提供します。PCVT と ISO は、GitHub のレポジトリからダウンロードいただくことが可能です。

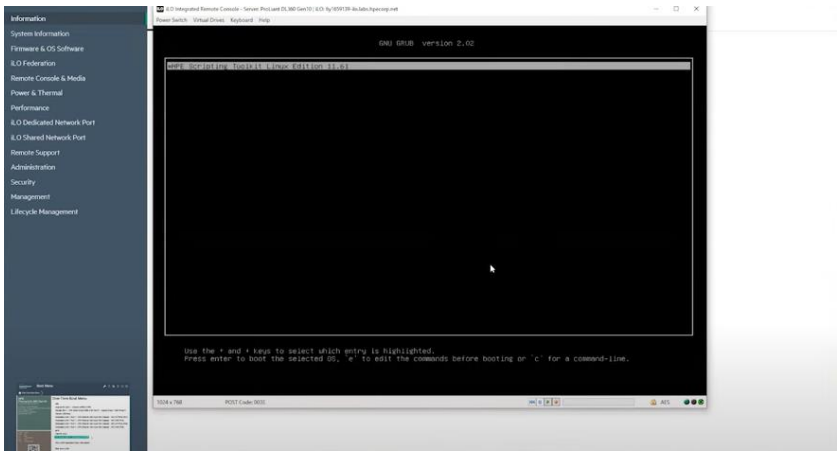
PCVT のデモ（改ざんをしていない状態）



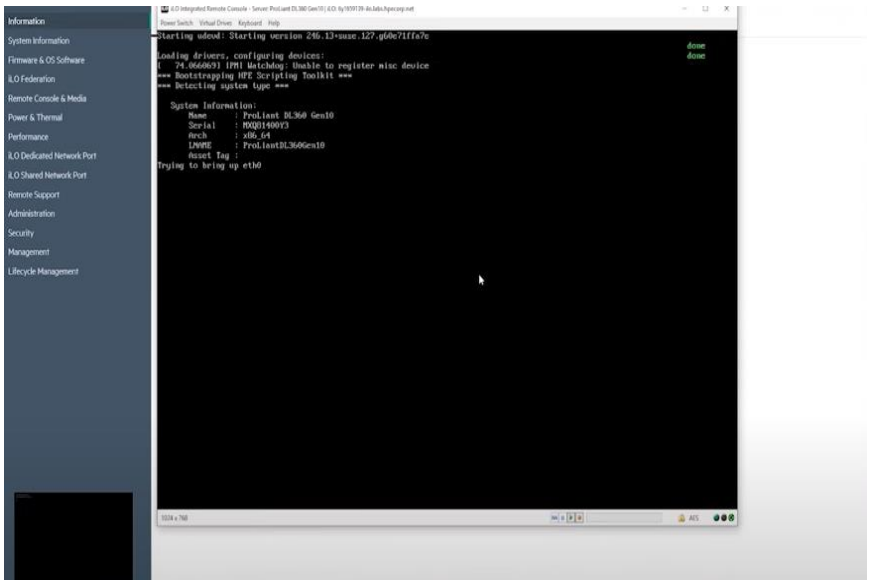
初めは、改ざんをしていない状態のデモをお見せします。



iLO の仮想メディアに ISO をマウントした状態で、ブートをします。

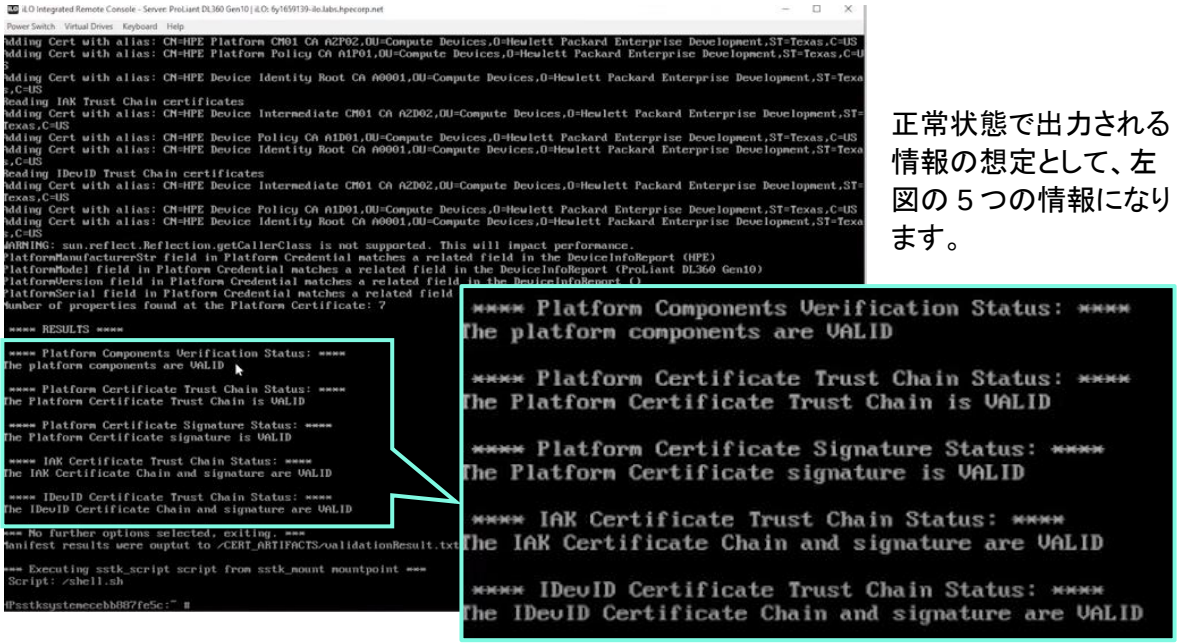


起動すると、左図のような画面が出ます。
「Enter」を押してイメージをロードします。



イメージが起動すると、以下が自動的にダウンロードされます。

- IAK
- IDevID
- iLO からプラットフォーム証明書
- 現在のサーバーハードウェアのコンテンツ状態を表したハードウェアマニフェストの世代
- PCVT 実行ファイル（現在のハードウェアのコンテンツの状態と、プラットフォーム証明書のコンテンツを比較するためのもの）



正常状態で出力される情報の想定として、左図の 5 つの情報になります。

① プラットフォームコンポーネント検証（ハードウェアマニフェストとプラットフォーム証明書を比較したもの）

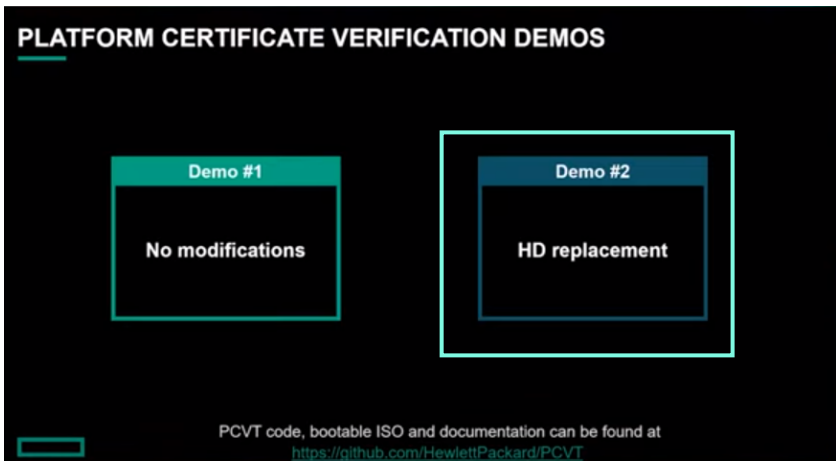
② プラットフォーム証明書のトラストチェーン検証

③ 証明書の署名検証

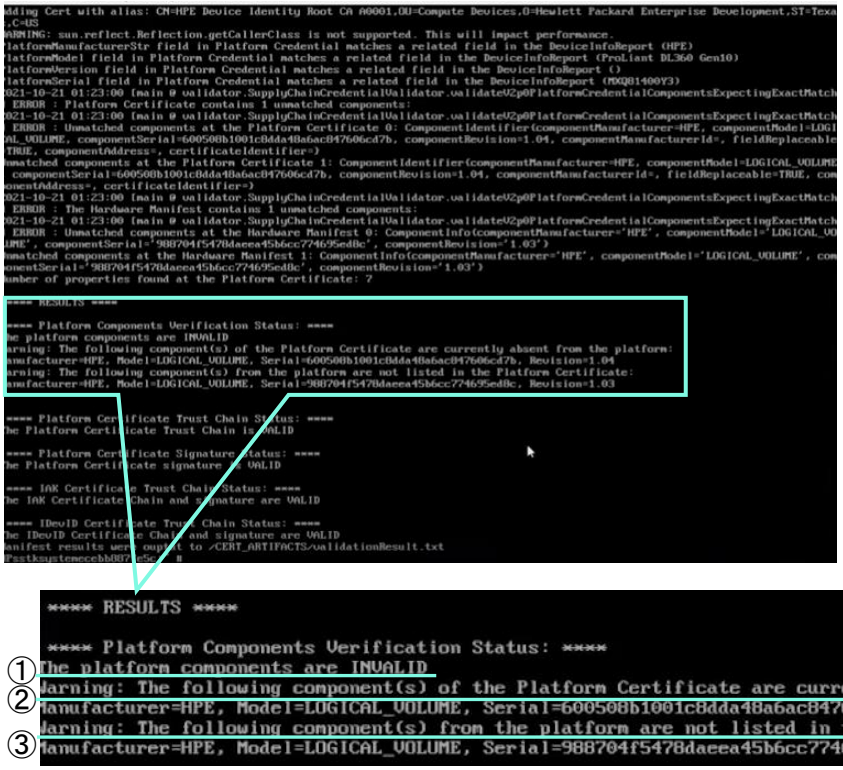
④ IAK 証明書のトラストチェーン検証と署名の検証

⑤ IDevID 証明書のトラストチェーン検証と署名の検証

PCVT のデモ（改ざんをした状態）



次に、ハードディスクを入れ替えた状態のデモをお見せします。



左図は、PCVT の ISO イメージを再実行した状態です。

① プラットフォームコンポーネント検証で、Invalid と表示されます。

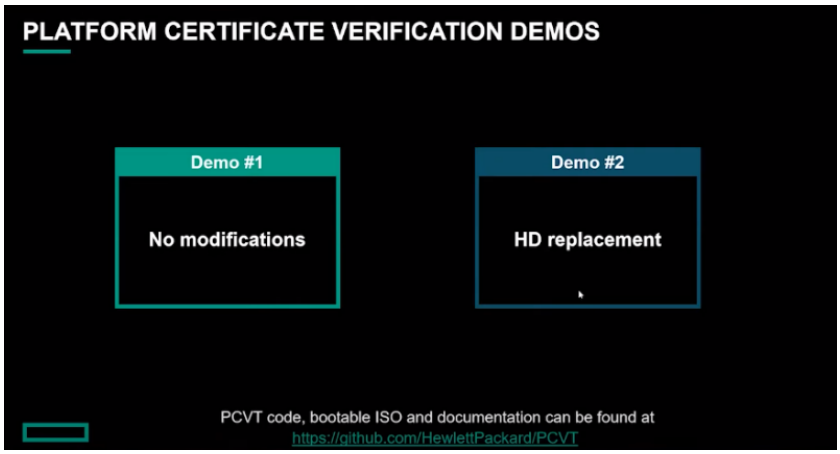
② プラットフォーム証明書に格納された内容のハードディスクが入っていないことが表示されています。

③ 現在入っているハードディスクがプラットフォーム証明書に入っている情報と一致しないことを表しています。

プラットフォームコンポーネント検証の判定

- 工場から出荷されたときは、あるコンポーネント（オリジナルのハードディスク）は存在していたが、今はそれがプラットフォーム上に存在しない
- プラットフォーム上にはコンポーネントが存在しているが、プラットフォーム証明書にはそのコンポーネントは存在しない。

詳細情報の入手



PCVT コード、ブータブル ISO、PCVT ドキュメントは、以下より入手可能です。

https://github.com/HewlettPackard/PCVT/releases/tag/pcvt_v1.0.1

以上