CEN TC 224

E-COMMERCE USING ELECTRONIC SIGNATURES IN JAPAN AND EUROPE

Keio University Tokyo – 4th July 2017

CEN Standards on remote signing

Franck LEROY – CEN TC 224 chairman, Protection Profiles expert

CEN TC 224

電子署名を利用した電子商取引の日本と欧州の事例と課題

慶応義塾大学　2017年7月4日

リモート署名に関するCEN規格

Franck LEROY – CEN TC 224 chairman, Protection Profiles expert

SERVER SIGNING SCOPE

- **The purpose of the trustworthy system (TW4S) is to create a digital signature under sole control of a natural person, or under control of a legal person which may be incorporated into an electronic signature or an electronic seal as defined in the eIDAS Regulation.**

- **SCOPE:**
  - provides commonly recognized functional models of TW4S;
  - specifies overall requirements that apply across all of the services identified in the functional model;
  - specifies security requirements for each of the services identified in the TW4S;
  - specifies security requirements for sensitive system components which may be used by the TW4S.

サーバ署名の範囲

- **信頼できるシステム（TW4S）の目的は、自然人の自らによる単独の管理、または法人の管理のもとで、eIDAS規則で規定している電子署名またはeシールに組み込むことができるデジタル署名を生成することである。**

- **対象範囲:**
  - TW4Sの一般に認められた機能モデルを規定する
  - 機能モデルの中で識別されているすべてのサービスに適用する全体的な要件を指定する
  - TW4Sで識別されている各サービスのセキュリティ要件を指定する
  - TW4Sが使用する可能性のある機密システムコンポーネントのセキュリティ要件を指定する

SERVER SIGNING OBJECTIVES

The objectives is to define requirements on the same scope as for a local signing device (pin/key/hash), but used remotely.

•Defines requirements to :

- the signing key protection and signing key usage;
- the signer authentication means and mechanisms;
- the link between the authenticated signer and the DTBS/R (hash);

サーバ署名の目的

サーバ署名の目的は、ローカル環境での署名装置（PIN/鍵/ハッシュ）と同じ対象範囲に関する要件を規定することであるが、サーバ署名の場合は署名装置を遠隔（リモート）で使用する。

•次について要件を規定する：

- 署名鍵保護および署名鍵使用
- 署名者認証手段およびメカニズム
- 認証された署名者とDTBS/R（ハッシュ）の間のリンク

CEN TC 224

EN 419 241 series

- **Response to the European Commission standardization needs on eIDAS interoperability framework and level of assurance**

- **Series of standard to define:**

  - 419 241 Part 1: General System Security Requirements

  - 419 241 Part 2: Protection Profile for QSCD for Server Signing

CEN TC 224

EN 419 241 シリーズ

- **eIDAS相互運用性フレームワークおよび保証レベルに関する欧州委員会の標準化ニーズへの対応**

- **次を規定する規格シリーズ**

  - 419 241 パート1: 一般システムセキュリティ要件
  - 419 241 パート2: サーバ署名のためのQSCD（適格署名生成装置）のプロテクションプロファイル

SOLE CONTROL ASSURANCE LEVEL

In order to fit to many scenarios as eSign/eSeal or simple/advanced/qualified, the server signing standard defines 2 levels of sole control.

•Sole control assurance level 1 (SCAL1):

- The signing keys are used, with a low level of confidence, under the sole control of the signer;
- The authorised signer's use of its key for signing is enforced by the SSA which authenticates the signer.

•Sole control assurance level 2 (SCAL2):

- The signing keys are used, with a high level of confidence, under the sole control of the signer;
- The authorised signer's use of its key for signing is enforced by the SAM […], in order to enable the use of the corresponding signing key

単独管理(SOLE CONTROL)保証レベル

電子署名/eシールまたは簡易/先進/適格のような様々なシナリオに対応するよう、サーバ署名規格は2つの単独管理(Sole control)レベルを規定している

•単独管理(Sole control)保証レベル 1 (SCAL1):

- 署名者自らによる単独の管理のもと、低い信頼性をもって署名鍵を使用する
- 署名者を認証するSSA(サーバ署名アプリ)が、認証された署名者の署名のための鍵の使用を実行する

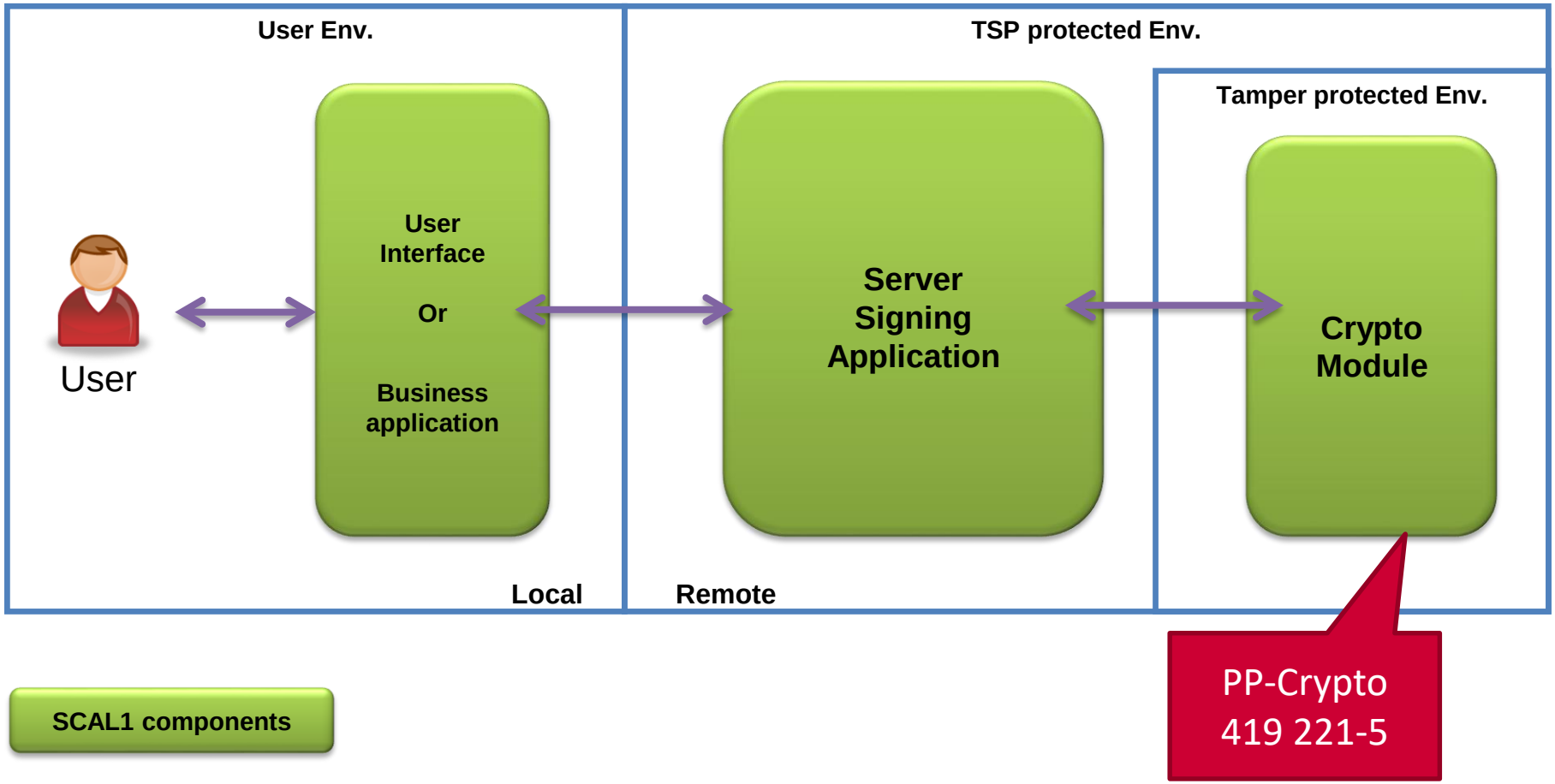
•単独管理(Sole control)保証レベル 2 (SCAL2):

- 署名者自らによる単独の管理のもと、高い信頼性をもって署名鍵を使用する
- 該当する署名鍵の使用を可能にするために、SAM(署名アクティベーションモジュール)が認証された署名者の署名のための鍵の使用を実行する

REMOTE SIGNING OVERVIEW

Sole control Assurance Level 1

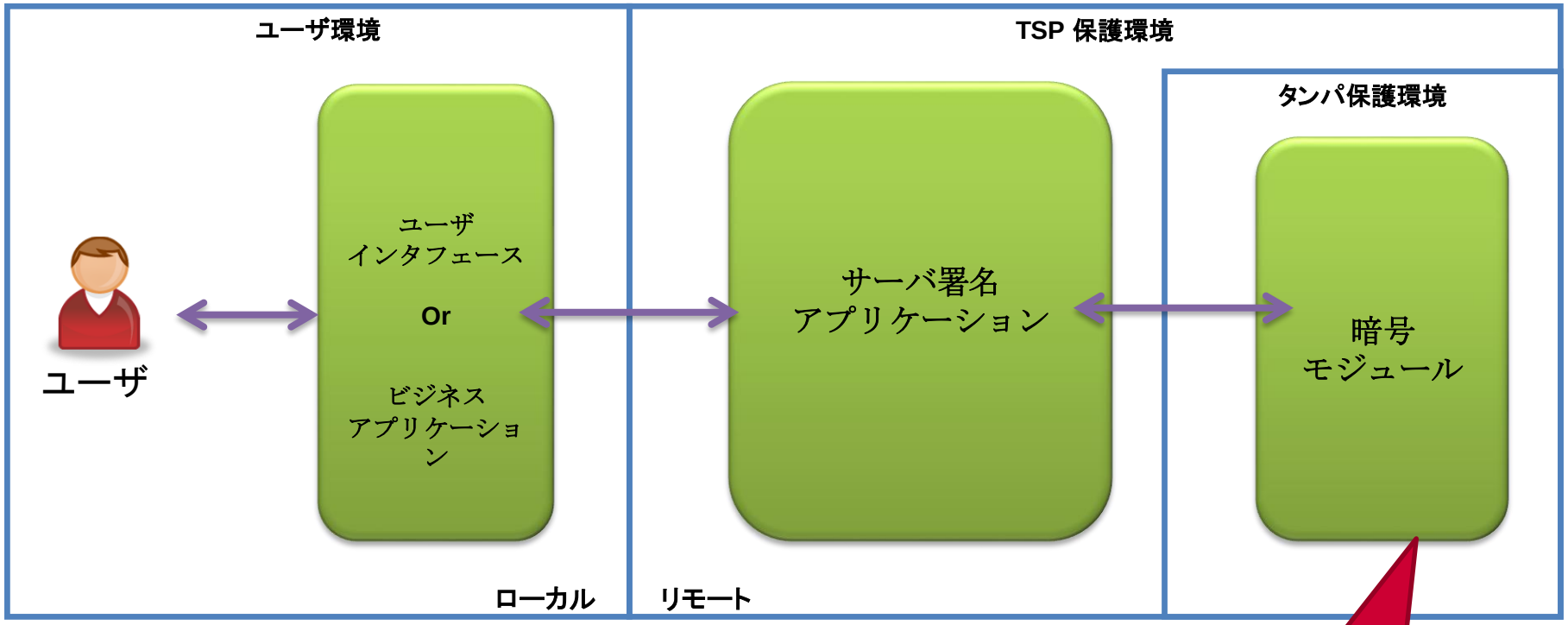
419 241-1
level1



リモート署名の概要

単独管理(Sole control)保証レベル1

419 241-1
level1



PP-Crypto
419 221-5

SCAL1 コンポーネント

データ通信

SIGNATURE ACTIVATION (SCAL2)

The goal for SCAL 2 is to provide the same level of security as provided by a smartcard. But the standard doesn't define an activation process, only security requirements on that process.

- **Signature Activation Protocol (SAP):**
  - The set of the necessary steps in order to create a signature;
  - Shall generates an 'activation data'.
- **Signature Activation Data (SAD):**
  - Shall be linked to the authenticated signer; (substantial level)
  - Shall be linked to the DTBS/R; (to protect from replay attack)
  - Shall be generated under sole control of the signer.
- **Signature Activation Module (SAM):**
  - Piece of software protected by an HSM;
  - Checks the validity of the SAD in order to activate the signing key.

署名アクティベーション (SCAL2)

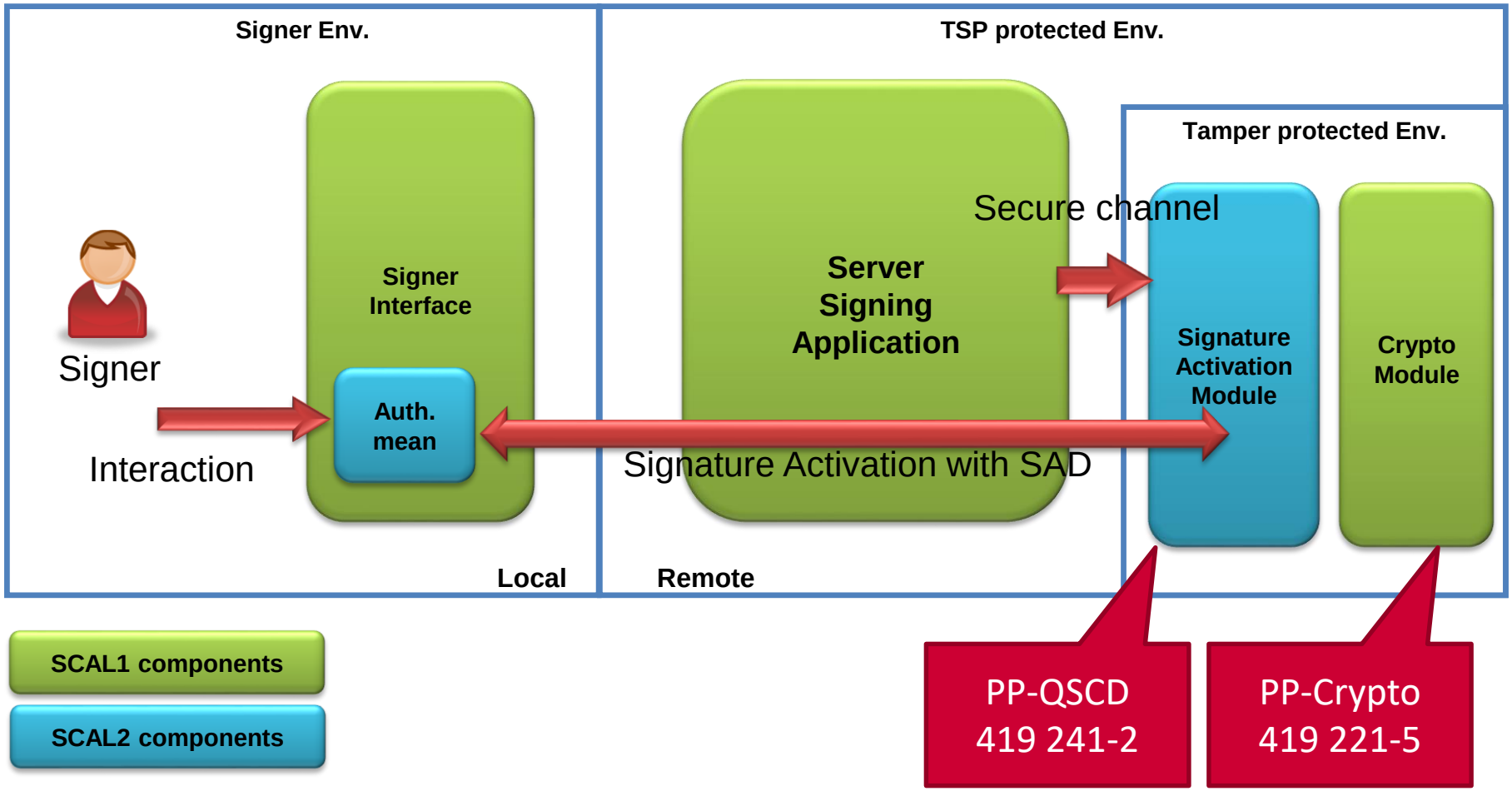
SCAL2の目的は、スマートカードと同じレベルのセキュリティを提供することである。ただし、当該規格はアクティベーションプロセスを規定しておらず、そのプロセスおけるセキュリティ要件のみを規定している。

- **署名アクティベーションプロトコル(SAP):**
  - 署名を生成するための必須ステップ
  - 「アクティベーションデータ」を生成する
- **署名アクティベーションデータ(SAD):**
  - 認証された署名者にリンクしている(Substantial(十分)レベル)
  - DTBS/Rにリンクしている(リプレイ攻撃からの保護)
  - 署名者自らの単独の管理のもとで生成する
- **署名アクティベーションモジュール(SAM):**
  - HSMによって保護されているソフトウェアの一部
  - 署名鍵をアクティベートするためにSADの有効性を確認する

REMOTE SIGNING OVERVIEW

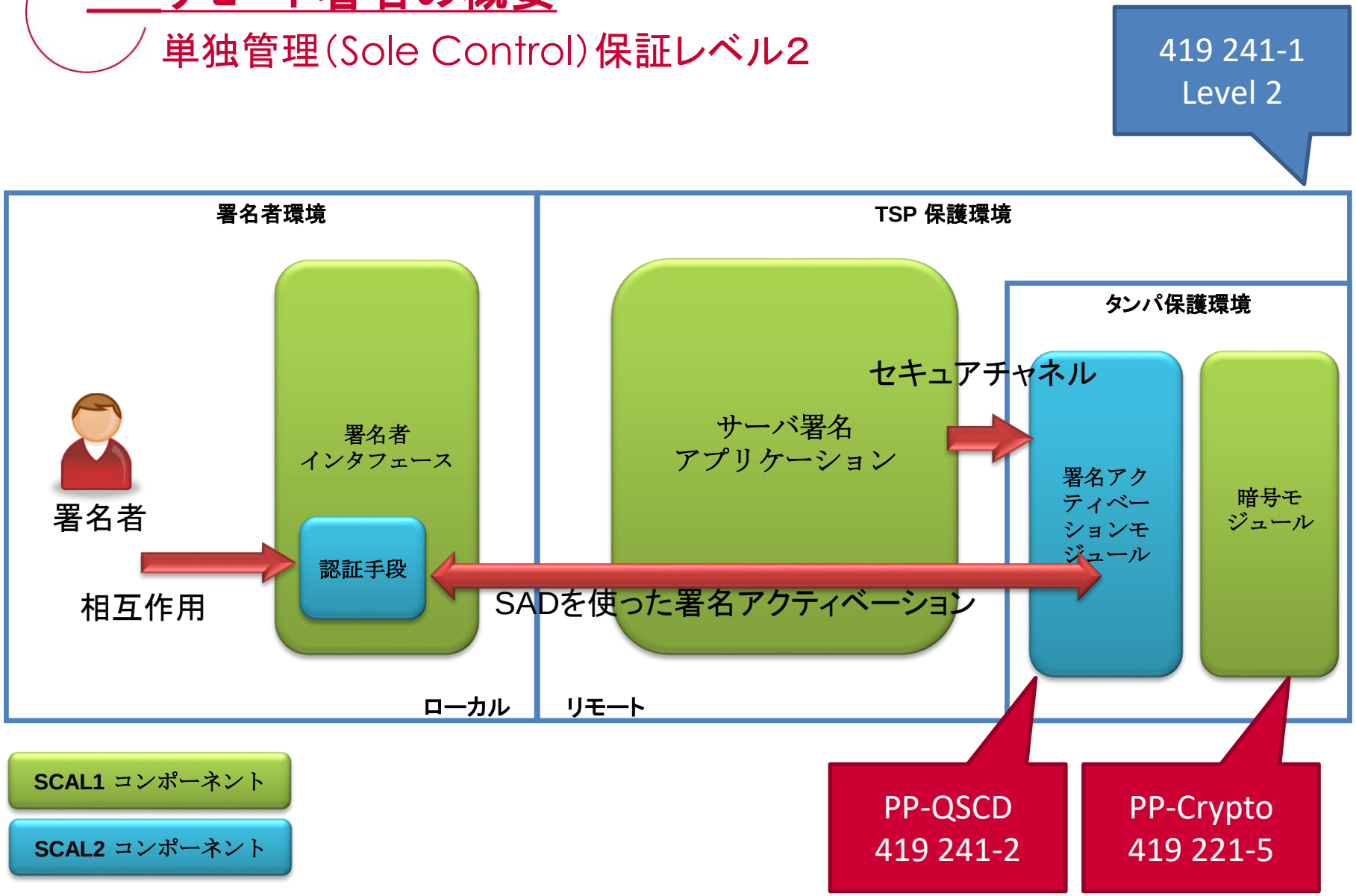
Sole control Assurance Level 2

419 241-1
Level 2



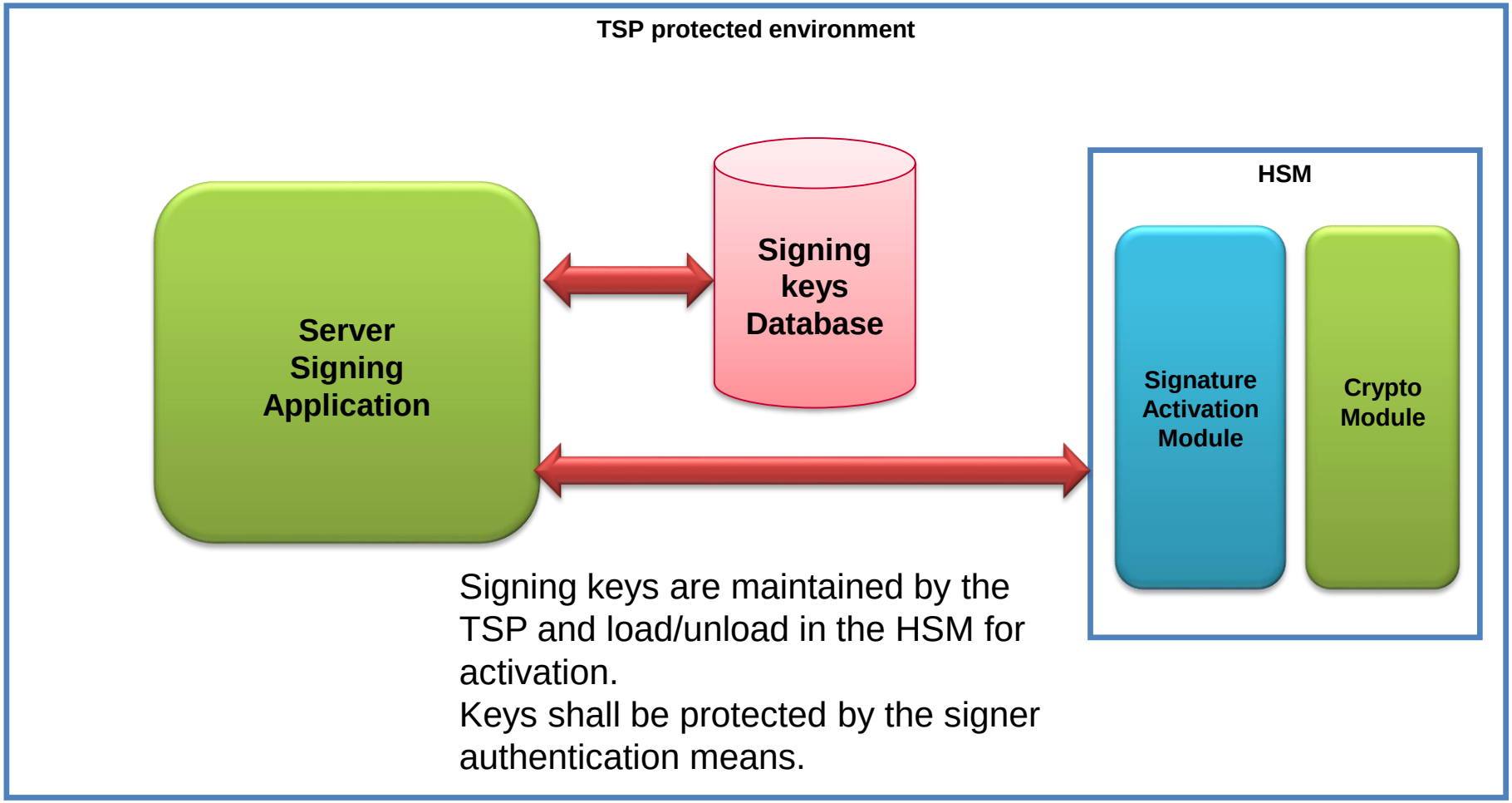
リモート署名の概要

単独管理(Sole Control)保証レベル2



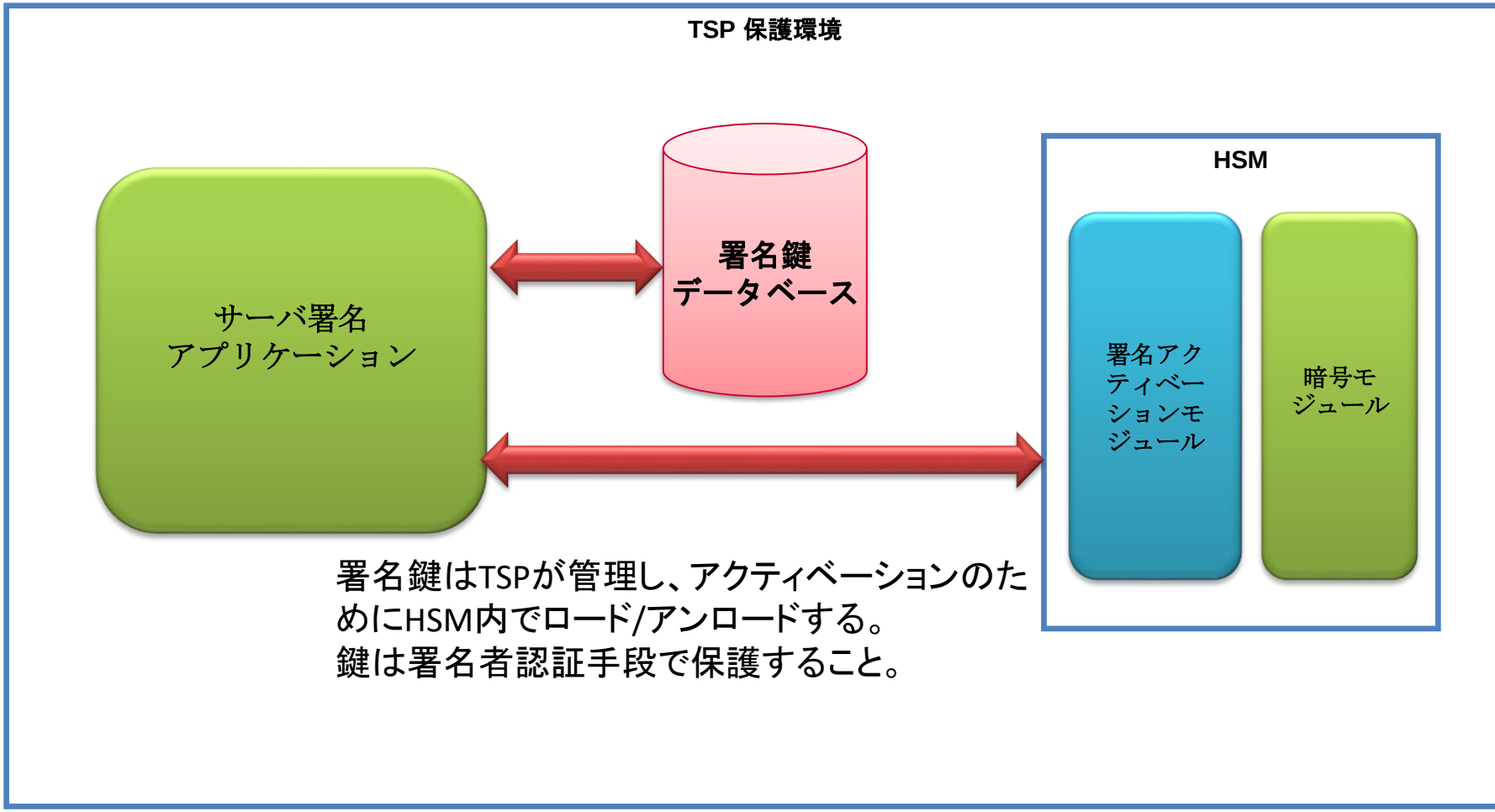
REMOTE SIGNING EXAMPLE

Long lived keys



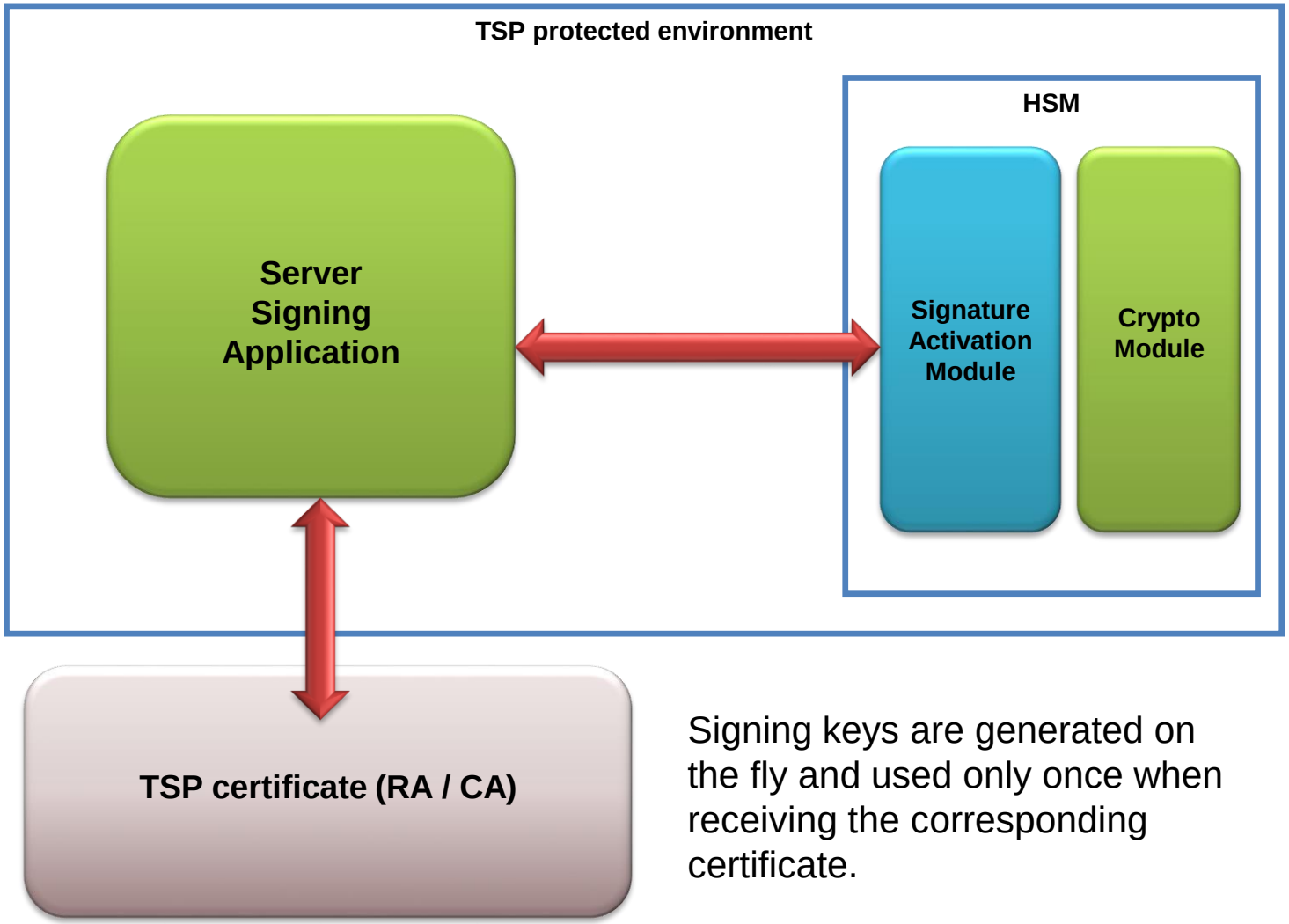
リモート署名の例

長期にわたって使用される鍵



REMOTE SIGNING EXAMPLE

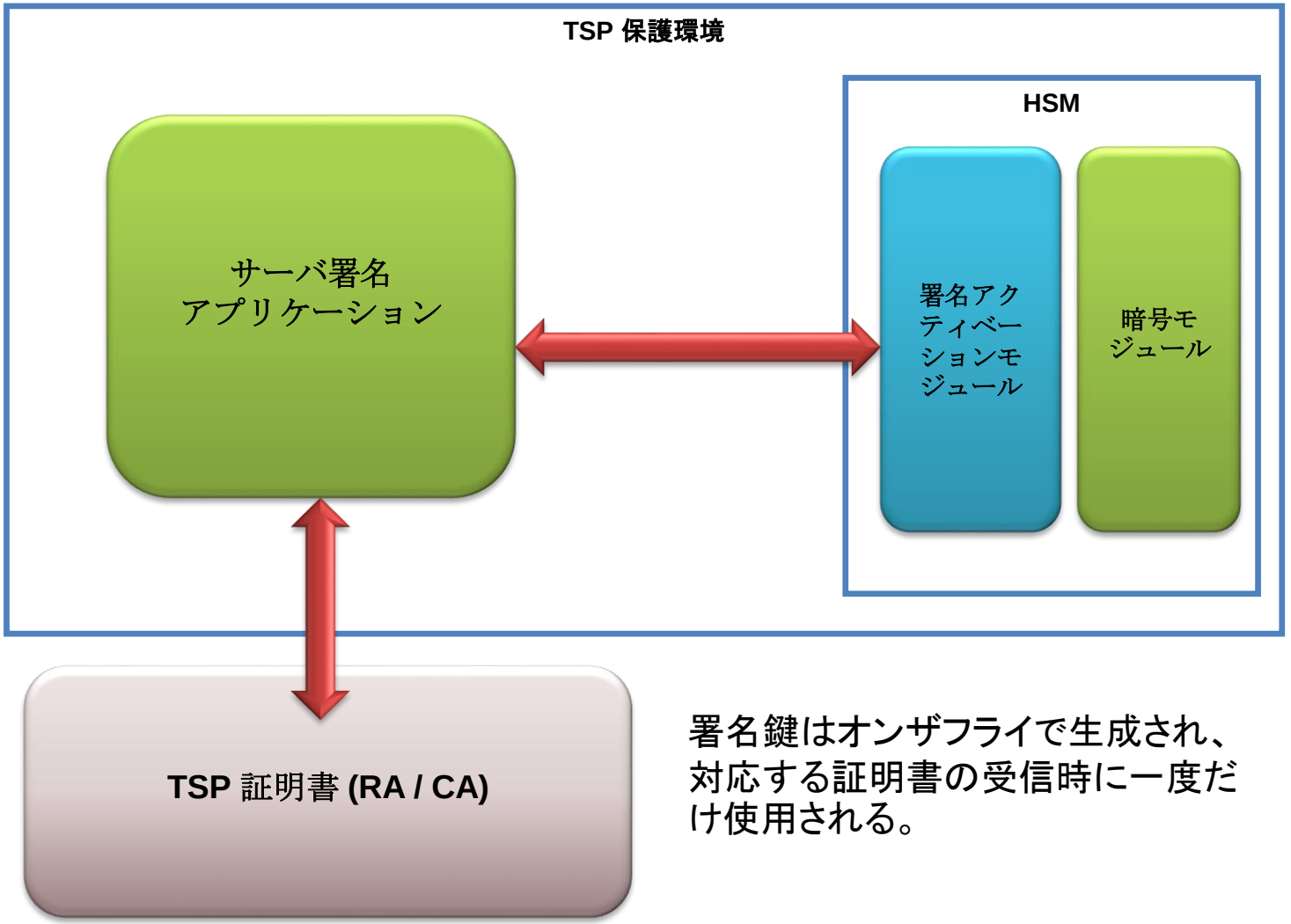
Short term keys



Signing keys are generated on the fly and used only once when receiving the corresponding certificate.

リモート署名の例

短期鍵

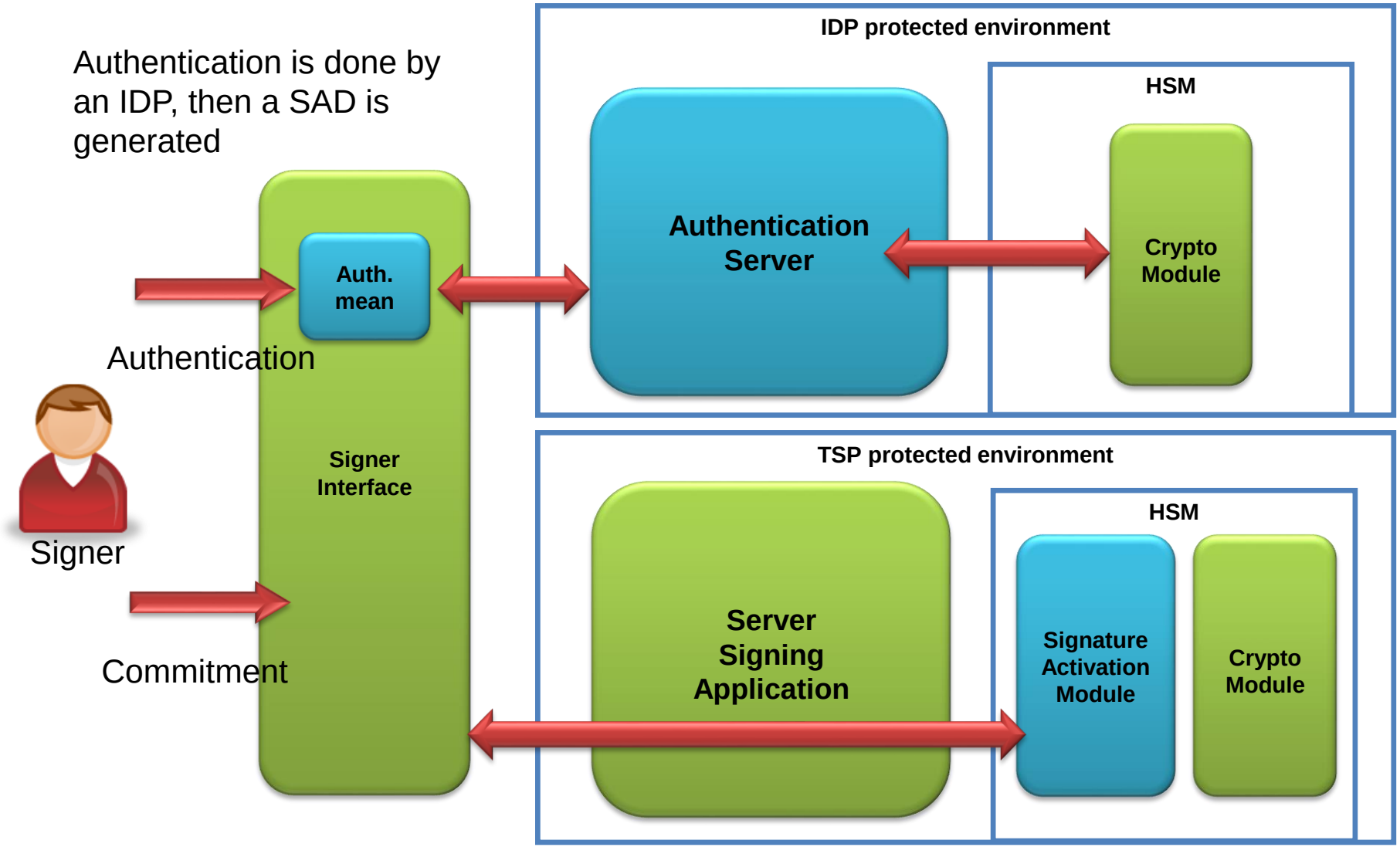


署名鍵はオンザフライで生成され、対応する証明書の受信時に一度だけ使用される。

REMOTE SIGNING EXAMPLE

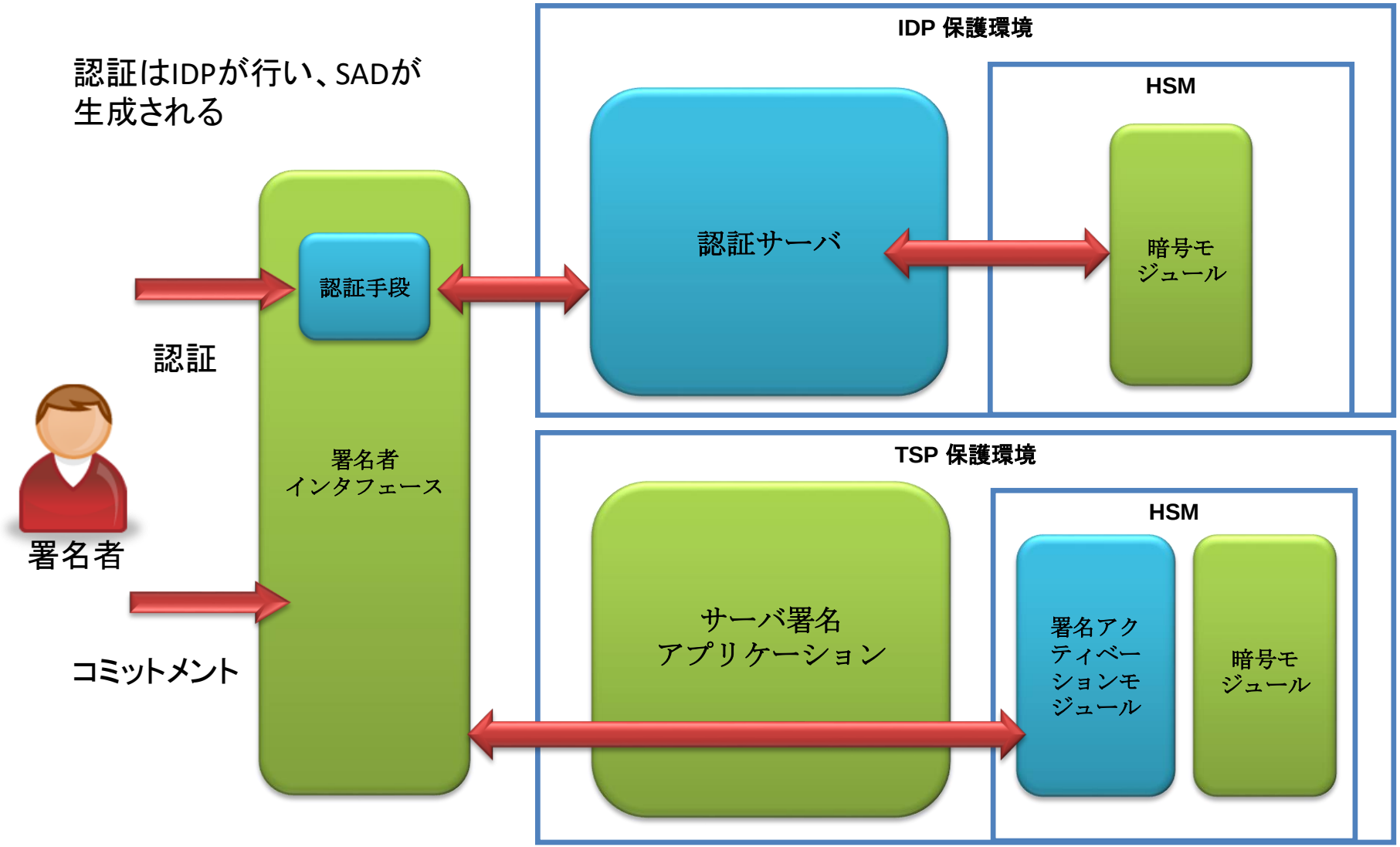
Delegation of authentication to an IDP

Authentication is done by an IDP, then a SAD is generated



リモート署名の例

IDPへの認証の委任



CEN STANDARDS ON REMOTE SIGNING

Conclusion

- **It is now possible to do remote signing based on EN standard**

- **Series of standard available soon :**

  - EN 419 241 Part 1: General System Security Requirements
    - Level 1: for electronic signature (or seal)
    - Level 2: for **Advanced** electronic signature (or seal)

  Approved by EU National Members on 22 June 2017

  - EN 419 241 Part 2: Protection Profile for QSCD for Server Signing
    - To qualify a signature device necessary for **Qualified** electronic signature (or seal)

  Under approval; vote on August 2017

リモート署名に関するCEN規格
まとめ

- **現在EN規格に基づくリモート署名を行うことが可能である**

- **規格シリーズは間もなく公開される予定である:**

  - EN 419 241 パート1：一般システムセキュリティ要件
    - レベル1:電子署名（またはシール）について
    - レベル2：**先進**電子署名（またはシール）について

    2017年 6月22日にEU加盟国により承認

  - EN 419 241 パート2：サーバ署名のためのQSCDのプロテクションプロファイル
    - **適格**電子署名（またはシール）のために不可欠な署名装置の限定

    承認中; 2017年 8月投票。

QUESTIONS ?

Contact information

THANK YOU !

Contact details:

Franck Leroy – Docapost/Certinomis CTO
Mobile : +33 6 59 67 73 09
Email : franck.leroy@docapost.fr

Web : www.certinomis.fr
Remote signing : https://www.certinomis.fr/cloud-signature

QUESTIONS ?
問い合わせ先

THANK YOU !

Contact details:

Franck Leroy – Docapost/Certinomis CTO
Mobile : +33 6 59 67 73 09
Email : franck.leroy@docapost.fr

Web : www.certinomis.fr
Remote signing : https://www.certinomis.fr/cloud-signature