

SC 27(情報セキュリティ)における バイオメトリクス関係プロジェクト

2014/10/7(火)

産業技術総合研究所

SC 27/WG 3エキスパート、WG 5委員

山田朝彦

目次

1. SC 27におけるバイオメトリクス関連プロジェクト
2. 現在進行中のバイオメトリクス関連プロジェクト
3. これから始まるバイオメトリクス関連プロジェクト

1. SC 27におけるバイオメトリクス関連プロジェクト

SC 27におけるバイオメトリクス関連PJの歴史

2003

WG 3 (セキュリティ評価技術)でISO/IEC 19792開始

2004

WG 2 (暗号とセキュリティメカニズム)でISO/IEC 24745開始

2005

WG 2でISO/IEC 24761開始

2006

WG 5 (アイデンティティ管理とプライバシー技術)設立

同時にISO/IEC 24745、ISO/IEC 24761移管

(ISO/IEC 19792は移管せず)

完了したバイオメトリクス関連プロジェクト

2009

24761 Authentication context for biometrics (ACBio)

WG 5 山田(日本)

生体認証結果の信頼性を判定可能なデータ構造の定義

19792 Security evaluation of biometrics

WG 3 Tekampe(ドイツ)、三村・大塚(日本)

ISO/IEC15408(CC)ではカバーできないバイオメトリクス特有の
セキュリティ評価(エラー率、脆弱性評価、プライバシー)

2011

24745 Biometric information protection

WG 5 Chun(韓国)

バイオデータの保護(管理策及び技術)

2013

24761 COR Authentication context for biometrics

WG 5 山田(日本)

ISO/IEC 24761の技術訂正(実装して判明した欠陥の修正)

他SCのプロジェクトとの関係

- 19792
 - SC 37 19795(精度評価)を参照
 - SC 37 30107 (*Presentation attack detection*)から参照
- 24761
 - SC 37 19784-1 Amd.3(BioAPI)で処理APIを定義
 - SC 37 19785-4 (CBEFF Part 4)セキュリティブロックでの扱い
 - SC 37 29164 (Embedded BioAPI)で処理APIを定義
 - SC 17 7816-11 で処理コマンドを定義

斜体字は現在進行中のプロジェクト、それ以外はIS化されたプロジェクト

2. 現在進行中のバイオメトリクス関連プロジェクト

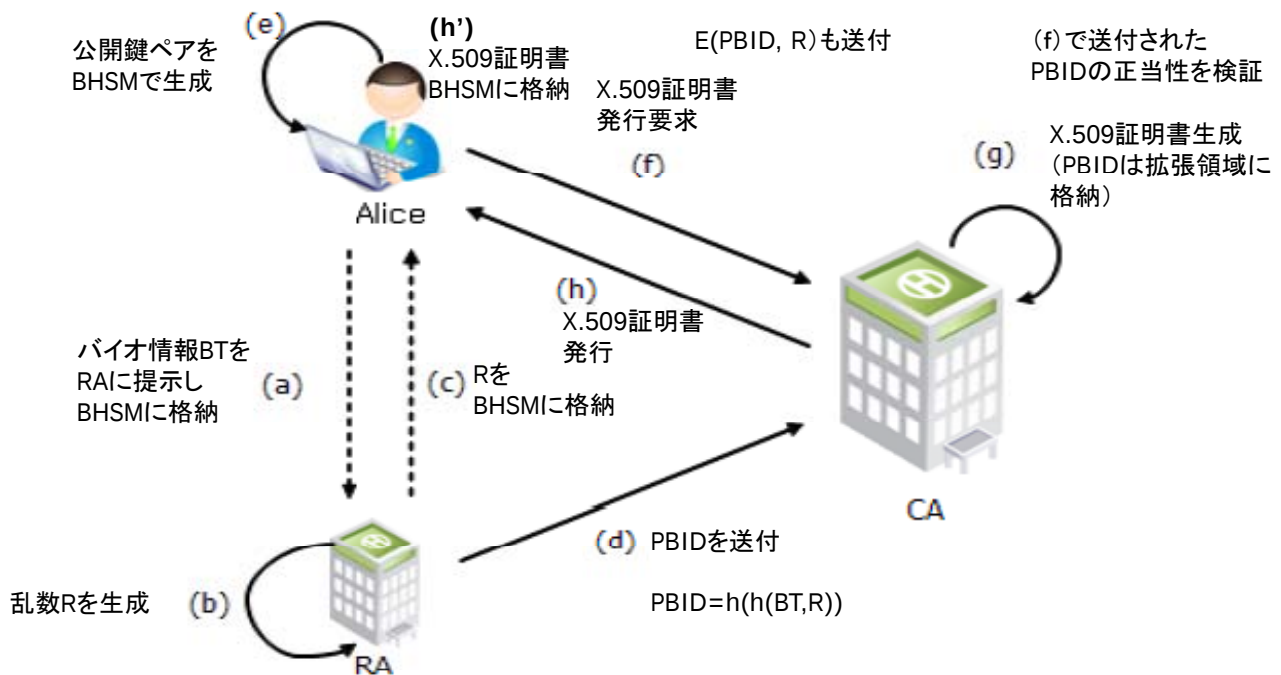
進行中のバイオ関連プロジェクト

17922 Telebiometric authentication framework using biometric hardware security module (ITU-T X.bhsm)

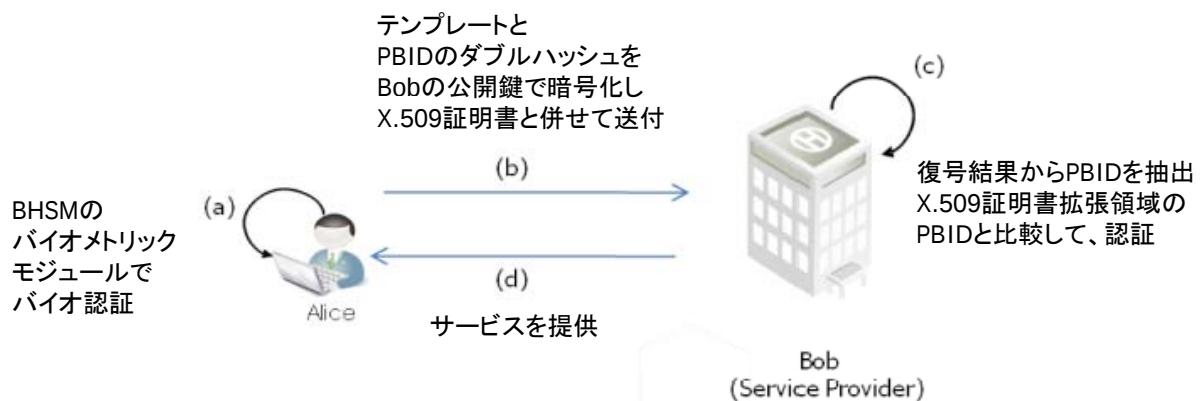
WG 5 Chun(韓国)

- 2012年2月開始
- 現在CD段階
- BHSM(Biometric hardware security module)とは
ひとつ以上のバイオメトリックセンサーを装備したバイオメトリック
モジュールとHSM(HWセキュリティモジュール)を一体化したHW
- PKIベースの認証において、テレバイオメトリック認証を使って、ユーザが
本人であることをVerifierにわからせたい
- スコープ
BHSMを使ったテレバイオメトリック認証の枠組み
BHSMを使ったテレバイオメトリック認証のメカニズム
上記のASN.1モジュール

BHSMを使ったテレバイオメトリック認証(登録) ーエディタオリジナル版ー



BHSMを使ったテレバイオメトリック認証(認証) ーエディタオリジナル版ー



17922 WDへの日本の貢献

WD 1

コメント数:19(ge:3、te:11)

他NB等のコメント数:2 ITU-T: 2(ge:1、te:1)

WD 2

コメント数:26(ge:3、te:11)

他NB等のコメント数:27 韓国:18(ge:1、te:4) 英:11(ge:5、te:1)

ISO/IEC 24761が適用可能であることを指摘し、寄書提出・採用

WD 3

コメント数:19(ge:4、te:13)

他NB等のコメント数:19 英:50(ge:14、te:9)

WD 4

コメント数:19(ge:1、te:15)

他NB等のコメント数:43 マレーシア:6(te:6) 英:37(ge:7、te:14)

17922 CD投票結果

賛成 13、反対 2(日・英)、棄権 27

コメント数: 日本 7(te:6) 英 13(te:8)

主なteコメント

1. (日)二重ハッシュを使う理由が衝突回避であるのは不適切
2. (日)バイOMETリックデータのフォーマットは19794を参照せよ
3. (日)そのまま適用できないのに、PKCS#10が適用できるかの記述あり
4. (英)登録の中でどの部分が対面かが不明確
5. (英)PBIDの意味が不明確

3. これから始まるバイオメトリクス関連プロジェクト

2014年10月から開始予定のプロジェクト

WG 3

Evaluation of presentation attack detection for biometrics

山田(日本)

2014年4月香港会議

SC 37 ISO/IEC 30107への貢献を目指したSPIは終了

継承PJをドイツが提案

2014年6月

最終的には日本から提案(PADのCC評価のための要件を規定)

2014年9月

賛成 16 反対 0 棄権 46 で成立

参加国: 日(エディタ)、仏(コエディタ)、独、英、米

WG 5

24761 Authentication context for biometrics

山田(日本)

定期見直しで改訂開始の予定

仕様の簡略化、適用範囲拡大を予定

ご清聴ありがとうございました