DICOMのセキュリティ

Lawrence Tarbox, Ph.D.
WG 14**議長**

ワシントン大学（セントルイス）医学部
マリンクロット放射線医学研究所

日本語訳：JIRA　DICOM委員会
高橋　智英

DICOMにおいて利用できるセキュリティ機構

- セキュアな情報交換
  - 通信チャネル
  - 媒体
- セキュアなオブジェクト
  - オブジェクトの機密性
  - デジタル署名
- セキュアなインフラ
  - 監査証跡
  - ユーザー識別情報の交換

セキュアな情報交換

- 目的
  - 相手認証
  - 通信におけるデータの完全性
  - 暗号化による通信の秘匿性
- 機構
  - セキュアなトランスポート接続プロファイル
    - 3DES方式によるTLS 1.0 (SSLから派生)
    - AES方式によるTLS 1.0
    - ISCL
  - セキュアな使用プロファイル
    - オンライン電子保存
  - セキュアな媒体プロファイル

セキュリティ通信プロファイル

- ISCL方式によるセキュアなトランスポート
  - ISCL規格（日本）に基づく
  - 対称暗号技術による認証
  - オンライン電子保存規格用に規定
- TLS方式によるセキュアなトランスポート
  - TLS 1.0の枠組み
  - RSA方式に基づく証明書を用いたピア認証
  - マスターシークレットの交換にRSA方式を使用
  - SHA-1ハッシュ関数による完全性の確認
  - トリプルDES EDE, CBC方式による暗号化
  - オプションとしてAES方式による暗号化（推奨）

AES方式によるセキュアなトランスポート

- 既存プロファイルとの後方互換
  - トリプルDESへのフォールバックを有効にした状態で、AES方式による暗号化をリクエスト
- AES方式を採用する理由
  - 独占的に所有されていない
  - 広く普及することが期待される
  - 3DESよりも効率が良い
    - 計算負荷が10%～30%
    - 特別なハードウェアを要さずに、100 Mbit／秒の暗号化と伝送が可能

VPNは？

- 現在、DICOMのプロファイルはない
- ただし、プライベートネットワークに関しては除外しない
  （ローカルポリシーの問題）

媒体のセキュリティ

- DICOMファイルの全体を保護
  - DICOMディレクトリーも含む
  - ファイルは暗号化された封筒に収められる
- 暗号メッセージ構文を利用
  - インターネット標準
  - 選ばれた受信者のみ開封できる
  - データの完全性を確認
  - 個々のファイルクリエータを識別
- 各種のセキュアな媒体保存プロファイル

オブジェクトの機密性

- 匿名化
- 属性レベルの暗号化

匿名化

理由

- ティーチングファイル、臨床治験、アクセス制御

方法

- 患者の識別情報を含むデータ要素を削除するだけ？
  - 例：HIPAAのセーフハーバー規則による

ただし、

- かかるデータ要素は数多く必要である

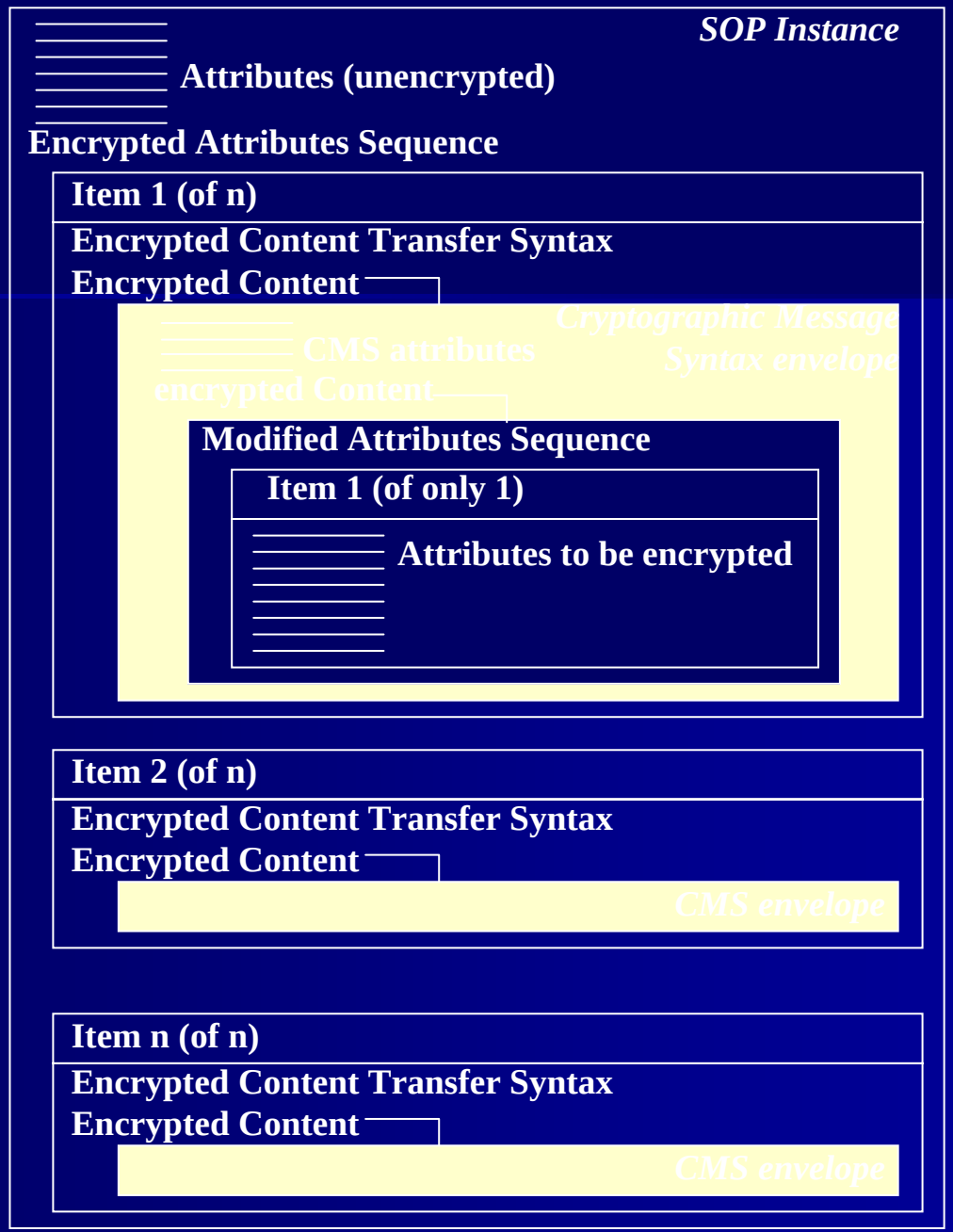
そこで、

- 削除する代わりに、架空の値で置き換える

属性レベルの暗号化

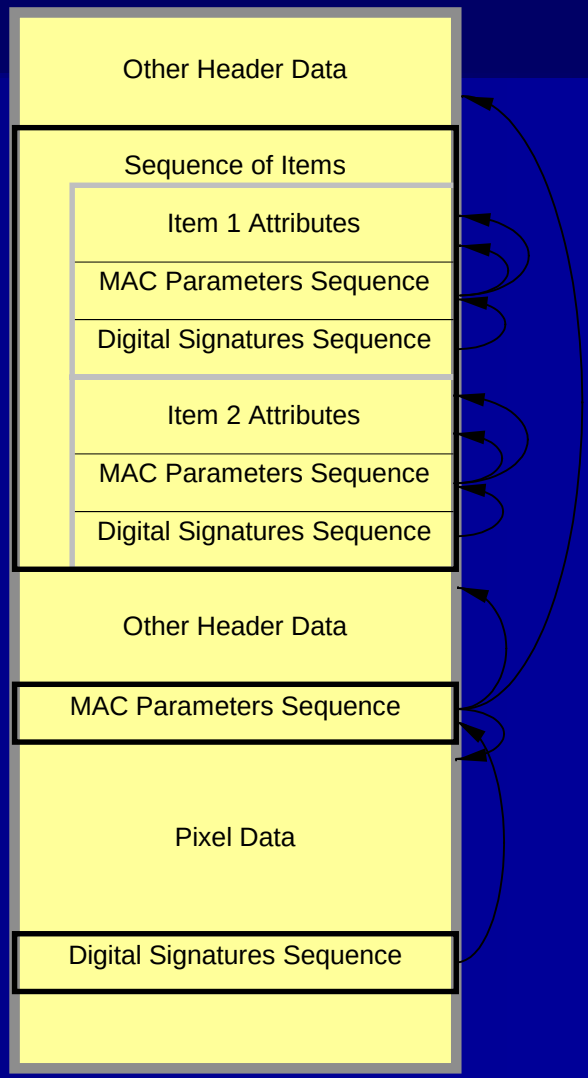
- 使用ケースによっては、元の属性値へのアクセス制御を要することがある為、
  - 元の値はCMS (暗号メッセージ構文) の封筒に保存することができる
    - データセットに埋め込まれる
    - 選ばれた受信者のみ開封できる
    - 受信者ごとに異なるサブセットを設けることができる
  - データの完全な復元が目的ではない

- 属性の機密性プロファイル


SOP Instance
Attributes (unencrypted)
Encrypted Attributes Sequence
Item 1 (of n)
Encrypted Content Transfer Syntax
Encrypted Content
Cryptographic Message Syntax envelope
CMS attributes
encrypted Content
Modified Attributes Sequence
Item 1 (of only 1)
Attributes to be encrypted
Item 2 (of n)
Encrypted Content Transfer Syntax
Encrypted Content
CMS envelope
Item n (of n)
Encrypted Content Transfer Syntax
Encrypted Content
CMS envelope

デジタル署名

- SOPインスタンスに埋め込まれる
- 有効期間中の完全性を確認
- 署名者を識別
- オプションとして、セキュアなタイムスタンプ
- 複数署名
  - 重複するサブセット
  - 複数の署名者
  - 個々の項目に署名
- **署名には目的がある！**

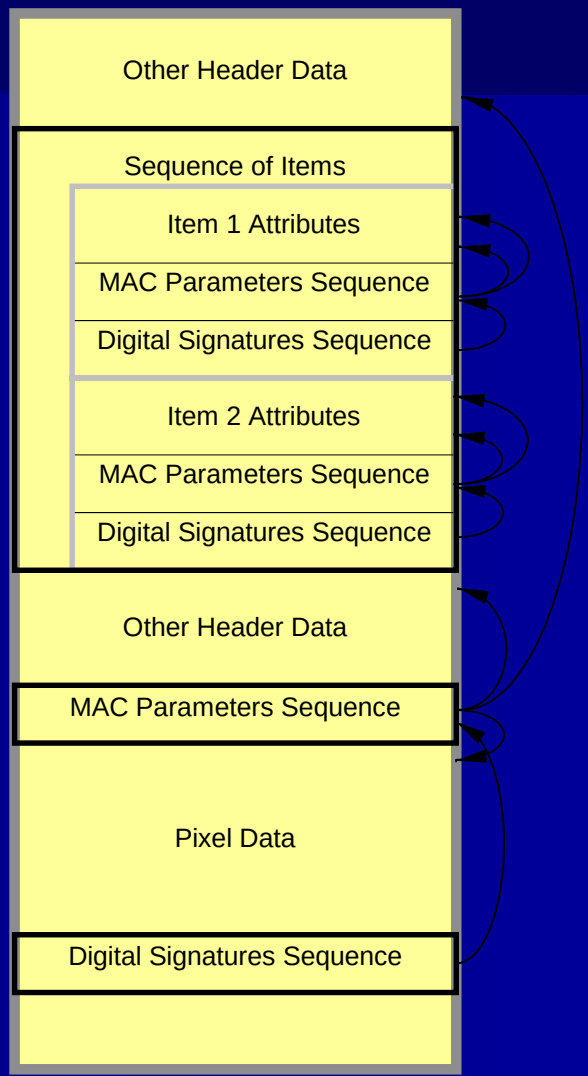


デジタル署名の目的

- 「目的」フィールドは署名者によって異なる（ASTM 1762規格より） 例：
  - 著者
  - 検証者
  - 閲覧者
  - 証人
    - 事象
    - 本人確認
    - 同意
  - 管理用

DICOMに埋め込まれた署名

- 選択された属性はデータセット内にある
- シーケンスは個々のエンティティとしてコード化される
- 各シーケンス内の項目には個別に署名できる



現行プロファイル

- セキュアな使用プロファイル
  - ベースデジタル署名
    - レガシーシステムが対象
      - 入力の際に照合
      - 出力の際に新規作成
  - ビット数保持デジタル署名
    - 今後、実施する可能性あり？
- デジタル署名プロファイル
  - ベースRSA（他のプロファイルにより参照される）
  - クリエータRSA（通常、機器）
  - 権限管理RSA（通常、オペレーター）
  - 構造化報告書RSA

SRデジタル署名

- 署名されるもの
  - SOPクラスUID
  - スタディおよびシリーズインスタンスUID
  - 全てのSR文書コンテンツモジュール
  - 現在のおよび関連のある証拠シーケンス
  - 「照合済み」になった後
    - SOPインスタンスUID
    - 照合フラグ
- 改訂内容は、新しいSOPインスタンス

セキュアな参照

- 既に署名されたオブジェクト
  - デジタル署名UIDおよび値を含む
- 署名されていないオブジェクト
  - 参照オブジェクト内の選択された属性のセキュアなハッシュを含む

  または
  - 参照オブジェクトのセキュアなハッシュを含む、その他の署名済みSRを参照する

SRデジタル署名に鍵を使用する場合

- 完全なセットを構成しているのは、何のオブジェクトか。アプリケーションには、これを知る手段があるか？

キーオブジェクト選択の拡張

- 新しい文書タイトル：
  - 完全なスタディ／取得コンテンツ
  - マニフェスト
  - 関連コンテンツ
- キーオブジェクト選択文書が他のキーオブジェクト選択文書を参照できるようにする（以前は許可されていなかった）

検討されたオプション

- MPPSは不可？
  - MPPSは、永続（複合）オブジェクトではない
  - MPPSは、署名済みの鍵オブジェクト選択文書の生成を引き起こしてしまう可能性がある
- Storage Commitmentは不可？
  - 現在いくつかのアプリケーションがStorage Commitmentと関連付けているセマンティックスを変更したくなかった

監査証跡の交換

- 監査証跡データを収集サイトに伝送
  - 長期保存を簡素化
  - 監視と解析を簡素化
- 必要性はDICOMの範囲を超える
  - HL7、DICOM、ASTM、IHE、NEMA、COCIR、JIRA、その他との共同作業？
  - 共通のベースフォーマット
  - 必要に応じて特殊化

混乱を解消しよう！

- ベースXMLのメッセージ形式が規定された（IETF RFC 3881）
  - 複数のドメインにより共有される
  - ボキャブラリ定義を使いやすくする必要あり
  - トランスポート機構は分かりにくい
- 補遺95は、DICOM特有のボキャブラリを示し、増やし、定義した
  - 補遺のスキーマを用いて、メッセージを作成し、DICOMの拡張を読む
  - 監査リポジトリーは、RFCのスキーマを用いて、鍵の解釈をすることができる
- プロファイルは、信頼性のあるシスログを要求する（IETF RFC-3195）

RFC-3195に関する背景情報

- 確実にBSDシスログに取って代わるもの
- BEEPメッセージ構造体、保存と転送のトランスポート、共通必須フィールド、およびXMLペイロードを提供
- 暗号化と署名のオプション

詳細度レベル

- サーベイランス
  - 個々の属性ではなく、スタディレベルでの詳細
  - 侵入を検出するよう設計された
- フォレンジック
  - かなり詳細になり得る
  - 発生過程を断定する

ユーザー識別情報ネゴシエーションの拡張

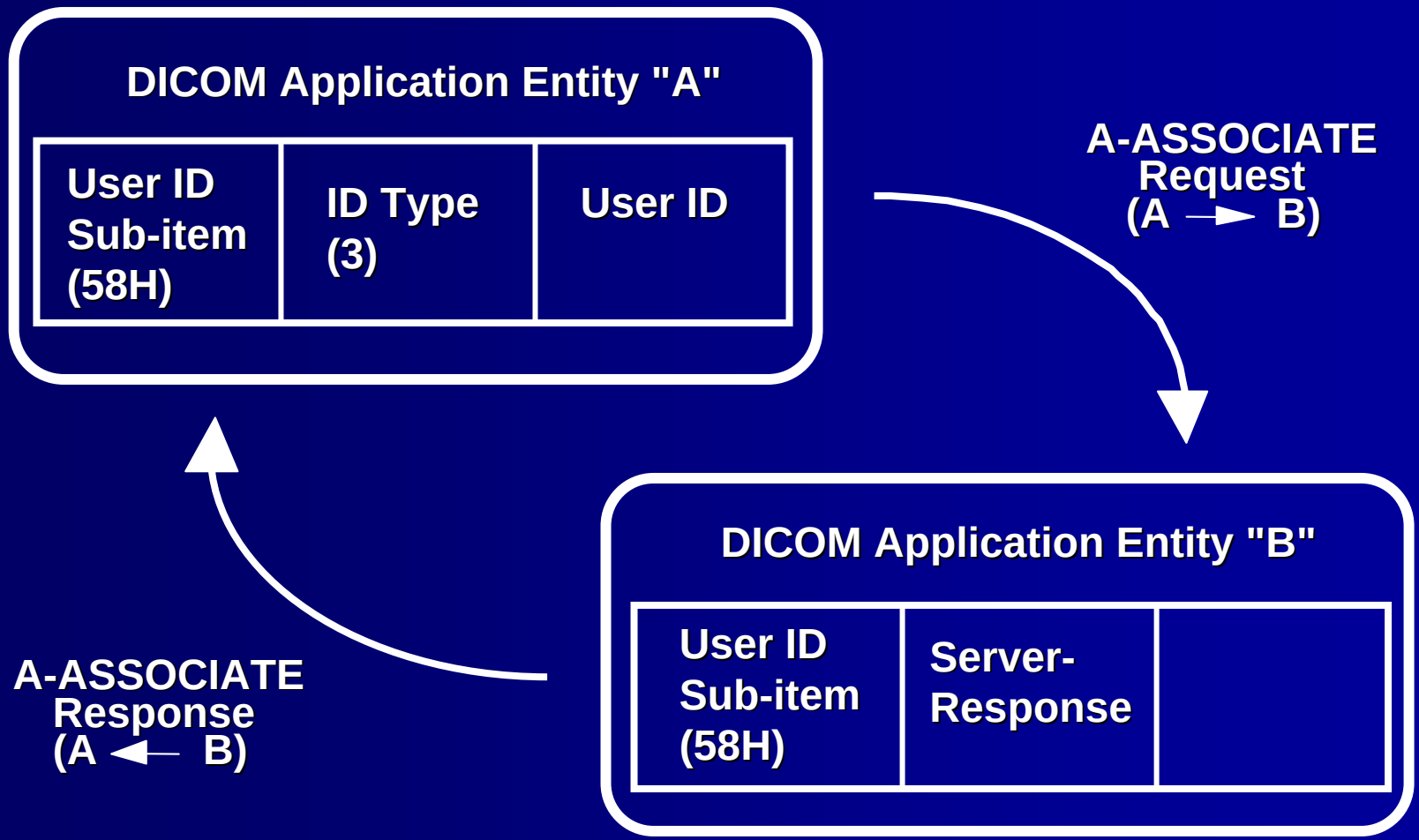
- 監査ロギングを容易にする
- システム間の権限およびアクセス管理に向かって前進
  - DICOMは依然としてアクセス管理をアプリケーションに委ねている
- クエリのフィルタリング
  - セキュリティならびに生産性の為

各種オプション

- ユーザー識別のみ、その他のセキュリティ機構なし
- ユーザー識別＋現行DICOMのTLS方式による機構
- ユーザー識別＋今後の低レベルのトランスポート機構 (例：セキュリティオプション付きIPv6)
- ユーザー識別＋VPN

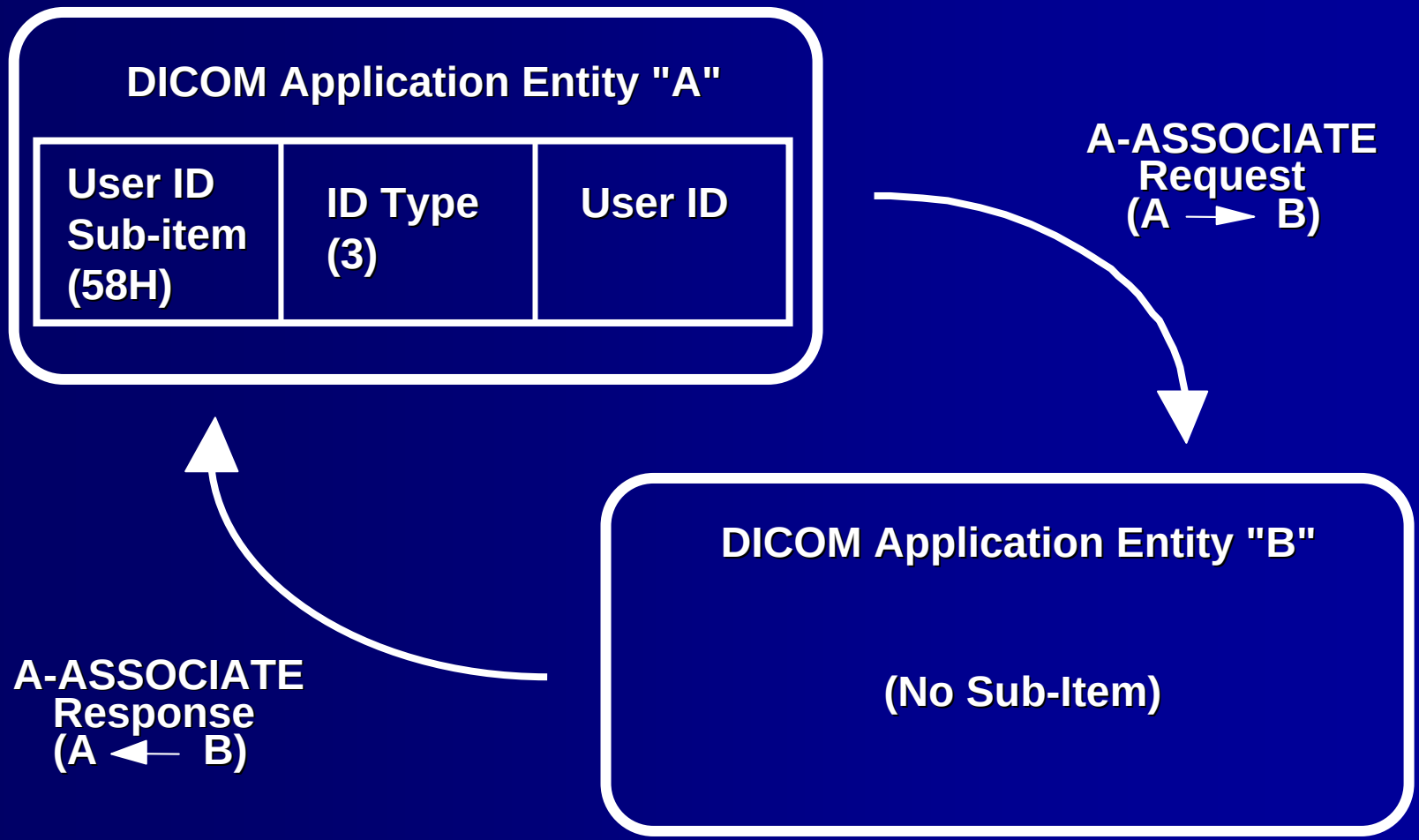
ネゴシエーションの拡張

レスポンスありの場合



ネゴシエーションの拡張

レスポンスなしの場合



IDタイププロファイル

- 未認証IDのアサーション
  - 信頼できる環境にあるシステム
- ユーザー名＋パスコード
  - セキュアなネットワークにあるシステム
- Kerberosに基づく認証
  - 最も高いセキュリティ

Kerberos

- Kerberosは、以下のような鍵配布センター [Key Distribution Center] (KDC) を採用している。
  - ユーザーを認証
  - ローカル ログイン プロセスに組み込むことができる
  - ローカル システムにチケット保証チケット[Ticket Granting Ticket] (TGT) を提供
- ローカル アプリケーションは、TGTを用いて、KDCにサービスチケットを発行させる。次いで、このチケットは、アソシエーション ネゴシエーション リクエストに送られる。
- リモート アプリケーションは、サービスチケットを用いて、ユーザーを確実に識別し、オプションとして、サーバーチケットを発行する。このチケットは、アソシエーション ネゴシエーション レスポンスに戻される。

今後に向けての準備

- 一方向のアサーション機構をサポートする機構は、サポートできると思われる（例：PKIとデジタル署名の使用）
- 二方向のネゴシエーションを要する識別機構は、サポートしない（例：リバティアライアンスによる提案）

今後のセキュリティ課題

- ノード間の完全なユーザー認証、鍵の管理
- 更に高度なアクセス制御のサポート
  - Role-based access
  - 施設アクセス　対　個人アクセス
  - 患者の権限管理
  - 対象受信者の一覧
- 新しい技術とアルゴリズムのサポート
- 今後の追加事項に関する提案を受け付けます！

皆様のご意見を歓迎します！

ありがとうございました。