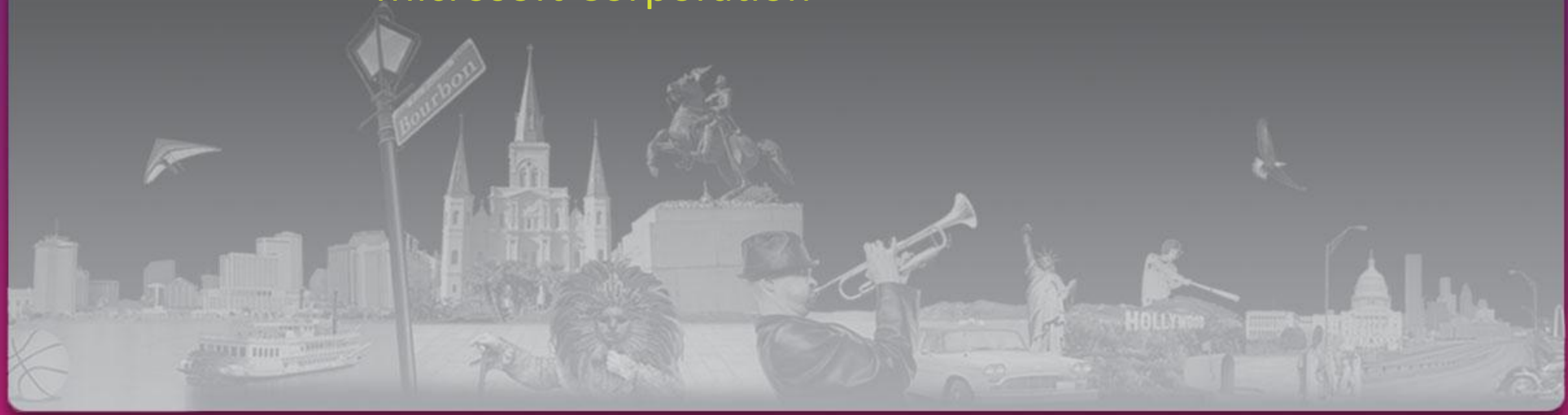
セキュリティ&プライバシーの課題とマイクロソフトU-Prove

渡辺清
Senior Security Architect and Consultant
Security Center of Excellence (SCOE), HQ Resource
Microsoft Corporation



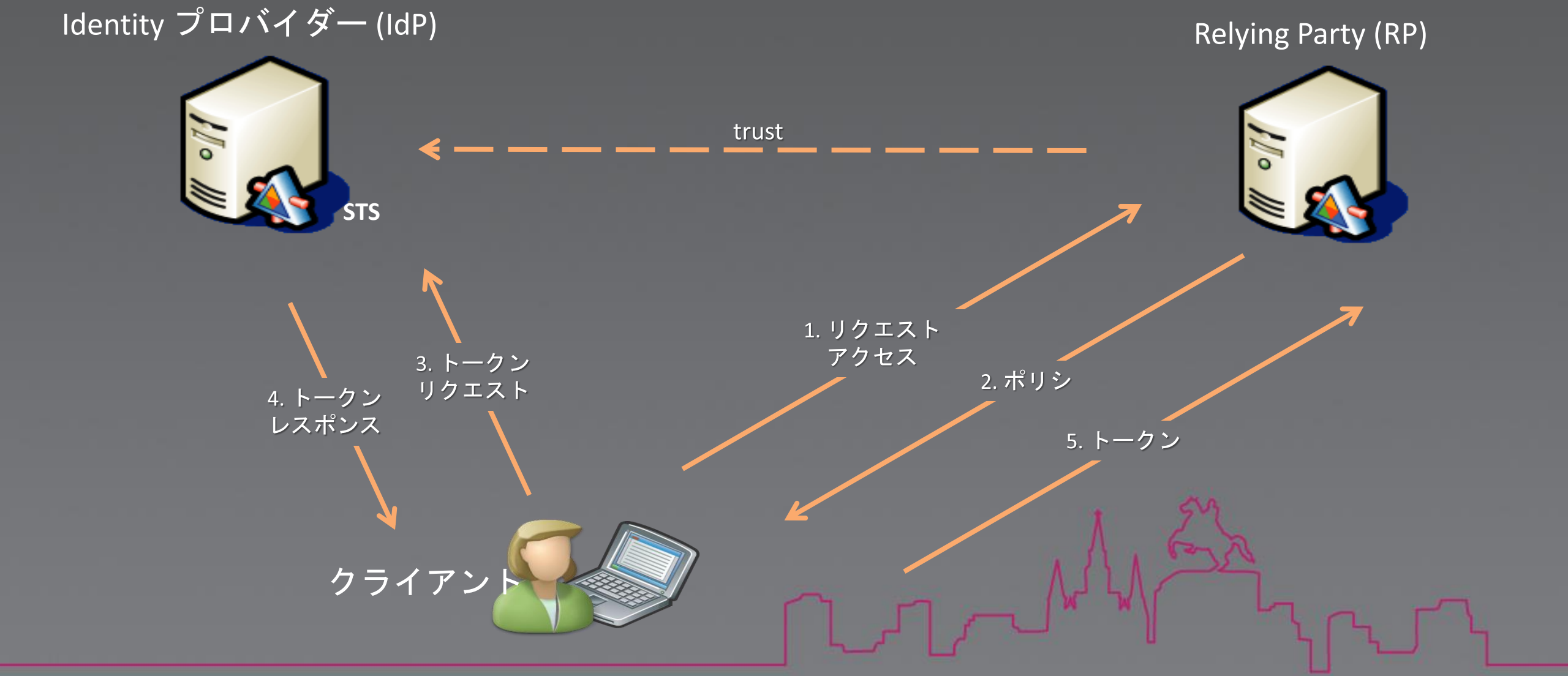
Identity現状

- 多くのサービスがオンラインへと移行する傾向にある
  - 利便性や使いやすさ
  - コスト
- 価値の高いトランザクションは、高いれレベルのidentifyの信頼性が必要となる
  - ユーザID/パスワードは普遍的であるが、低いレベルのセキュリティしか提供しない (NIST's LoA)
  - 典型的な"企業向け"ソリューション (例えば ケルベロスやPKI(?))はスケールアウトせず、インターネットを考慮したシステムには十分に柔軟性があるとは言えない。
  - どうやって現実社会のIDをオンラインで利用できるのだろうか？

Identity フェデレーション(連携)

- 一番有名なアーキテクチャ
  - 柔軟性
  - 簡単に展開
  - 多くのプロトコル: WS-Federation/Trust, SAML, Information Cards, OpenID, OAuth, …
- 但し多くの課題が存在
  - セキュリティ
  - プライバシー
  - スケーラビリティ

フェデレーションアーキテクチャ



課題#1: セキュリティ

- IdP クレデンシャルが危殆化し、全てのRPにアクセスできる
  - フィシング問題
- Idpに対して強化された認証は可能だが、RPに対する認証は弱い
  - 発行されたトークンはソフトウェアベースのみ（トークンハイジャックアタック等）
- IdP は大きなセキュリティホールになり得る
  - IdP (インサイダ攻撃やウイルス攻撃) こっそりとユーザに成りすまし
  - アクセスを拒否することも可能

課題#2: プライバシー

- IdPはユーザ活動をプロファイルできる
- IdPはどのRPを訪問したのか分からないかもしれないが、結託してプロファイリングは可能
  - タイミングによる相関分析
  - ユニーク値による相関分析 (例えば、電子署名、シリアル番号)

課題 #3: スケーラビリティ

- 全てのトークンは、オンデマンドで取得
  - IdP は24/7で稼動する必要がある
- IdPは、単一障害ポイント
  - DOS攻撃の格好のターゲット
- IdPは、各ユーザアクセスのボトルネックとなってしまう

U-Prove技術

U-Prove 技術

- 暗号技術とPKIセキュリティとID連携(Federation)の柔軟性を組合し、プライバシーを設計段階から組み込む
- 様々なタイプの電子クレデンシャルや資格ドキュメントに利用可能となる

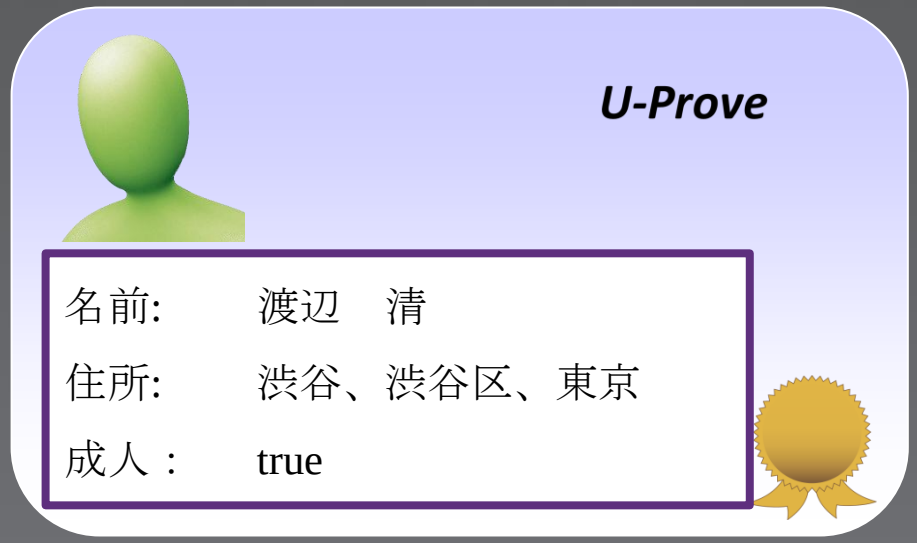
- “典型的な”暗号トークン (X.509証明書、 SAML , Kerberos チケット) よりユニークなセキュリティ、プライバシー、効率性の利益を持ち合わせている

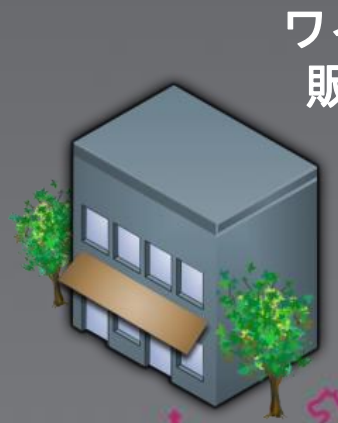
何が新しいの? 最低限の公開!

- U-Prove トークンは、必然的に結論に達する相関関係の情報を持たない
  - トークン発行とその中身はリンクしない

- ユーザは、エンコードされたクレームのサブセットのみを公開
  - RPから予期しないリクエストに対して実施
  - トークンの完全性を保持しないがら実施

最低限の公開とは？





最低限の公開とは？


政府
成人で東京都民と証明しなさい
本当に東京都民の成人ですか？
ワイン販売
U-Prove
名前: [redacted]
住所: [redacted] 東京都
成人: true

X.509との比較

- 公開鍵は、By Designで公開され、ユニークIDとなりえる
- CAは、この公開鍵を署名する
- RPは、署名を検証するために、この公開鍵を利用する
- X.509の属性は、証明書に格納され、いつも提示される（隠せない）
  - 国民ID等。。。

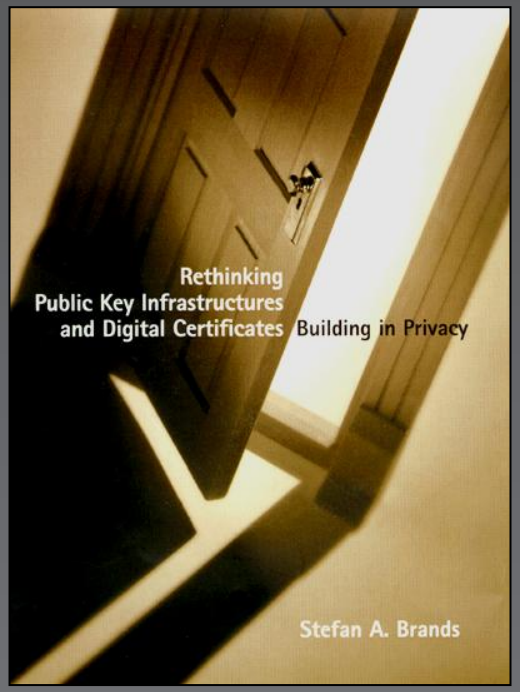
- U-Proveは、プライバシーがBy Designで組み込まれる
  - アプリケーションは、公開鍵を利用するが、この情報を隠すことができる。
    - X.509では通常可能ではない。

マジック？

- 署名検証を成功させながら、どうやって情報を隠すのか？
  - 全ての属性情報は、トークン署名の中でエンコードされる
  - ユーザは、属性情報をエンコードして署名生成、署名検証はそのエンコードされた情報から実施する
- どうやって公開鍵を隠すのか？
  - Blinding 技術
    - 発行者(CA)は、公開鍵の派生したメッセージを署名する。
    - ユーザは、追加の操作をし、blinding factorを取り除き、新しい署名を作成する。この情報がRPによって検証される
    - 発行者(CA)は、本当の公開鍵や署名は分からない。

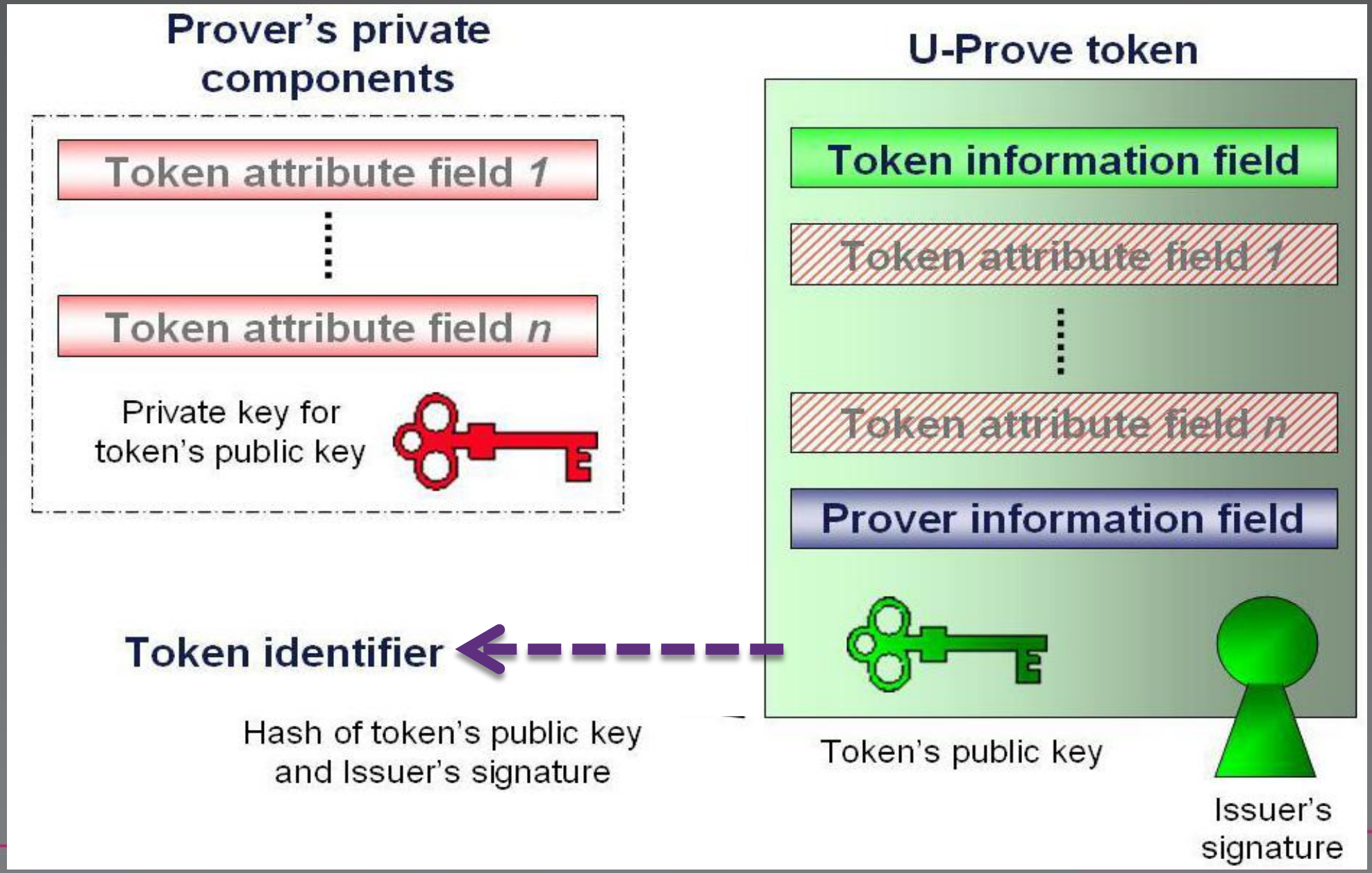
利用される暗号とは

- Brands protocolsに基づく
  - 30以上の論文
  - PKIの発展
  - MIT Press book, Ron Rivestによる推薦

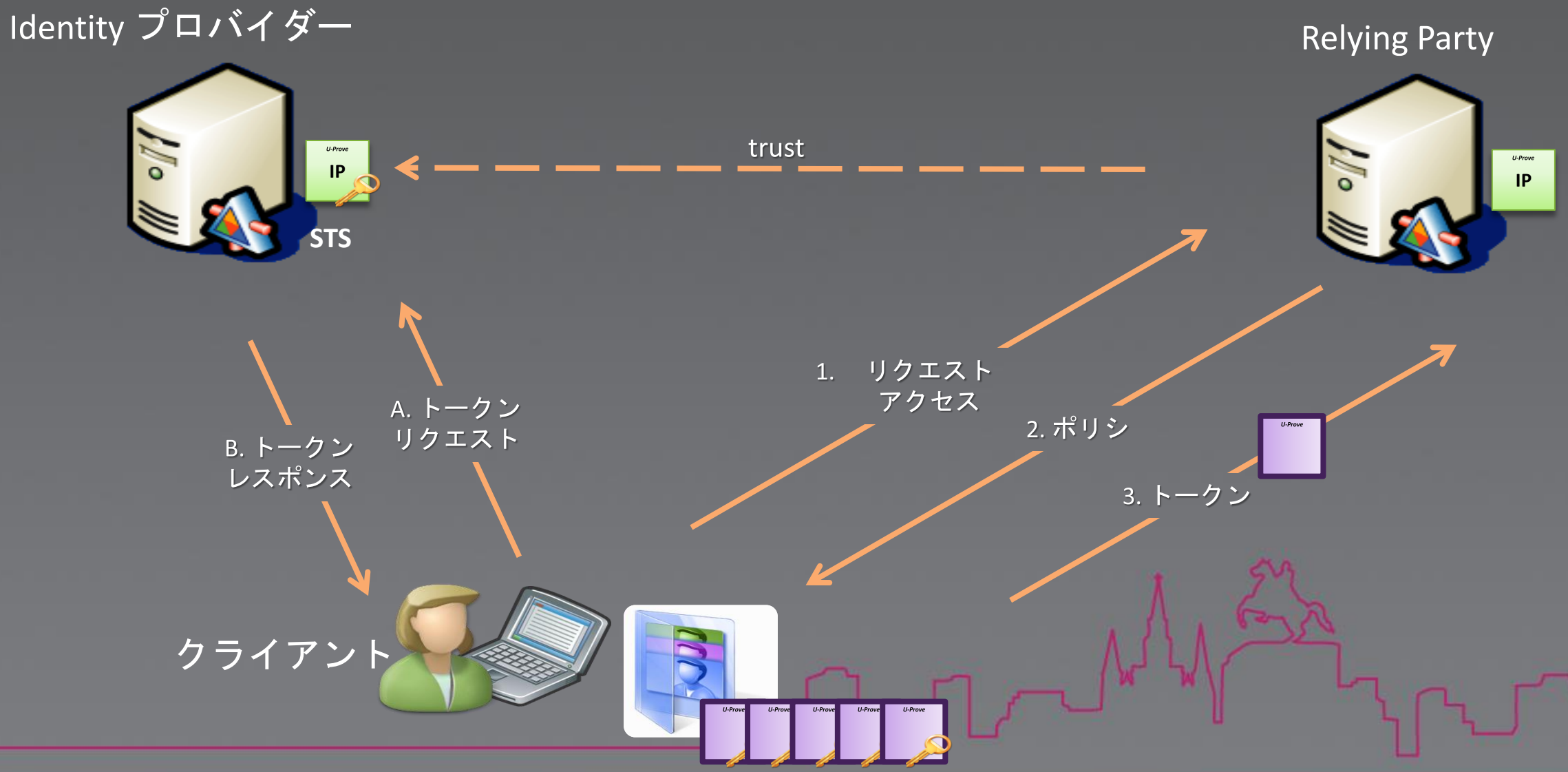


- 発行は “restrictive blind signature”を利用
  - 発行者は属性は知りえるが、トークンの最終的な公開鍵(Public Key)と署名(Signature)は見えない
- トークン提示時は、“proof of knowledge”を利用
  - 情報の公開せず、“secret”を提示
  - Schnorr protocolを利用して生成

U-Prove V1.0 トークン詳細



ID連携 + U-Prove

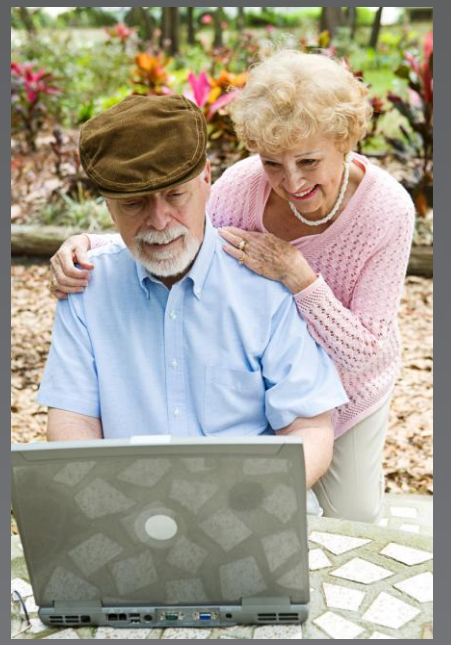

Identity プロバイダー
Relying Party
U-Prove
IP
STS
trust
U-Prove
IP
1. リクエスト
アクセス
2. ポリシ
3. トークン
A. トークン
リクエスト
B. トークン
レスポンス
クライアント
U-Prove

まだ実装されていないU-Prove機能

- Device保護トークン
- Privacyを保護する失効
- 属性プロパティの証明
- 制限利用トークン
- ゼロ知識トークン提示
- 等々

マーケット

- E-Government (国民ID)
- E-Health (レコード管理)
- クラウドコンピューティング
- 文書署名(最低限公開)
- 広告 (プライバシーを考慮した広告プラットフォーム)
- E-Cash
- ソーシャルネットワーキング

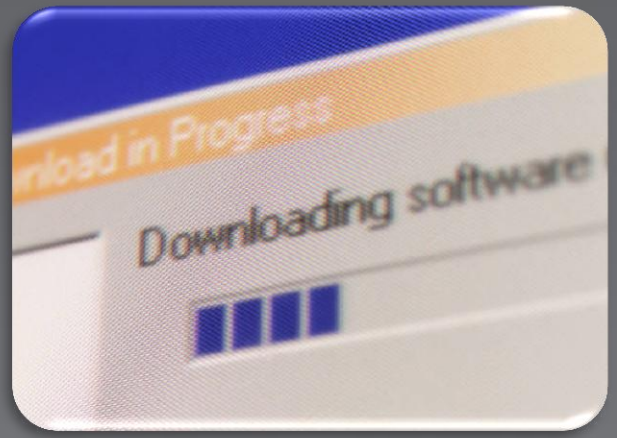


課題とU-Proveの貢献

U-Prove CTP

U-Prove Community Technology Preview

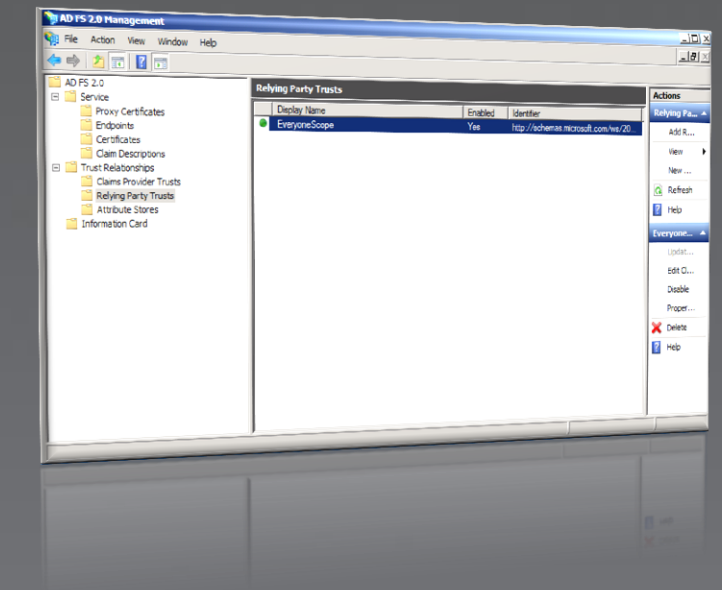
- 仕様 (Open Specification Promise)
  - U-Prove crypto 仕様
  - IDメタシステム仕様への統合
- オープンソース crypto SDKs (crypto仕様の実装)
  - Code Galleryにポスト, BSDライセンスの使用
  - C# と Javaバージョン
- Microsoft製品に利用
  - Windows CardSpace 2.0
  - Windows Identity Foundationに統合
  - Active Directory Federation Services 2.0



http://www.microsoft.com/u-prove

Microsoft productsへの統合

- Windows Identity Foundation
  - U-Prove issuer key management
  - IdP のU-Prove を理解する STS
  - RPのU-Prove token handler
- Active Directory Federation Services 2.0
  - IP-STS
  - RP-STS
- Windows CardSpace 2.0
  - U-Prove が利用できる information card
  - U-Prove トークンの保存、取得、提示



Fraunhofer FOKUS / Microsoft デモ

ドイツ eID card

VIDEO

デモアーキテクチャ

OKS 登録

Offene Kommunikationssysteme OKS Technische Universität Berlin

Windows Server 2008 R2

Active Directory Federation Services 2.0

E-Book

Bücher online

Microsoft .NET | Windows Identity Foundation

OKS Feedback

Offene Kommunikationssysteme OKS Technische Universität Berlin

Microsoft .NET | Windows Identity Foundation

1. オンライン登録、カードの取得

2. 登録されたIDを提示, e-bookをオンラインで閲覧

3. 匿名でフェードバックを残す

ドイツ nPA card

Windows CardSpace 2.0

WIF 設定（U-Prove用)

Register the U-Prove WIF Extension in the application web.config

```
<compilation>
  <assemblies>
    …
    <add assembly="Microsoft.IdentityModel.UProve, Version=3.5.0.0, Culture=neutral,
     PublicKeyToken=31BF3856AD364E35"/>
  </assemblies>
</compilation>
…
<microsoft.identityModel>
  <service>
    <serviceCertificate>…</serviceCertificate>
    <securityTokenHandlers>
      <add type="Microsoft.IdentityModel.UProve.Tokens.UProve.PresentationTokenHandler,
         Microsoft.IdentityModel.UProve, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
        <issuerParametersStore type="SampleIssuerParametersStore, UProveUtil, Version=1.0.0.0, Culture=neutral" />
      </add>
    </securityTokenHandlers>
    <audienceUris>…</audienceUris>
  </service>
</microsoft.identityModel>
```

AD FS 2.0設定(U-Prove用)

Use PowerShell to setup the server

```
# Enable the EveryoneScope
Enable-ADFSRelyingPartyTrust -TargetName EveryoneScope

# Adjust the lifetime of issued U-Prove tokens
# Set-ADFSRelyingPartyTrust -TargetName EveryoneScope -TokenLifetime 11520

# Adjust the number of U-Prove tokens issued
# Set-ADFSProperties -DisconnectedTokenCount 25

# Generate Issuer parameters and private key (valid for 5 years)
Set-ADFSIssuanceParameters -Lifetime 1825.00:00:00.00

# Export signed Issuer parameters
$ipLocation = "c:¥users¥public¥issuance.xml"
Export-ADFSIssuanceParameters -Path c:¥issuerparams.xml

# Update the information card to support for U-Prove tokens
Update-ADFSInformationCard
```

Question?

U-Prove リソース

- ビデオ:
  - Scott Charney’s RSA アナウンス: http://www.rsaconference.com/2010/usa/recordings/keynote-catalog.htm
  - 概要: http://channel9.msdn.com/shows/Identity/Announcing-Microsofts-U-Prove-Community-Technical-Preview-CTP
  - 技術概要: http://edge.technet.com/Media/Learn-what-Microsofts-U-Prove-release-is-all-about
- U-Prove Community Technology Preview:
  - ダウンロード: http://www.microsoft.com/u-prove
  - 開発者向けビデオ: http://channel9.msdn.com/shows/Identity/U-Prove-CTP-a-developers-perspective/

Microsoft®