



# Privacy-Preserving Multi-Dimensional Credentialing Using Veiled Certificates

Chin-Tser Huang\*      John H. Gerdes, Jr.

\*Department of Computer Science and Engineering  
University of South Carolina

Computer Science and Engineering @ University of South Carolina



## The Problem

- Organizations often use common personal identifiers (PIs) to satisfy reporting obligations and uniquely identify the same individuals, thereby making it possible to cross-link and aggregate the transactions of the same person from multiple sources
  - For example, SSN has been used as student ID, employee ID, insurance plan ID, ...

Computer Science and Engineering @ University of South Carolina



## The Problem

- On the other hand, if the information systems in organizations are breached, the adversary can use the unique PIs to search and obtain sensitive information belonging to specific individuals
  - Individuals trust the organizations that they will store sensitive data securely, which the organizations may fail to fulfill



## The Idea

- The underlying problem is that individuals have lost control over their own PIs
  - Organizations must capture the PI to satisfy reporting obligations
  - However once individuals disclose their PI to the organization they lose control over how it is used
- We introduce the **veiled certificate (VC)** to address the problem
  - VC allows individuals to maintain control over their personal information while satisfying the regulatory and reporting needs of today's security conscious environment
  - It is the only known credentialing approach that supports anonymous multi-dimensional credentialing



## Desirable Certificate Properties

Desirable Certificate Characteristic	Required Properties	Interested Constituent
<ul style="list-style-type: none"> <li>Credentials created in a secure, verifiable manner</li> </ul>	<ul style="list-style-type: none"> <li>Non-forgable, verifiable certification.</li> </ul>	Consumer of Certificate
<ul style="list-style-type: none"> <li>Prevent misuse of the certificate (e.g., identity theft)</li> </ul>	<ul style="list-style-type: none"> <li>Detect collusion – sharing single ID among multiple individuals</li> <li>Prevent pooling of different people's certificates</li> <li>Allow aggregation</li> </ul>	
<ul style="list-style-type: none"> <li>Support credential revocation</li> </ul>	<ul style="list-style-type: none"> <li>Allow credential revocation for cause</li> </ul>	
<ul style="list-style-type: none"> <li>Suitable for establishing accountability &amp; audit trail</li> </ul>	<ul style="list-style-type: none"> <li>Support an audit trail that can link actions to a single, identifiable individual</li> <li>Allow access to individual's identity in case of illegal activities or breach of contract</li> </ul>	



## Desirable Certificate Properties

Desirable Certificate Characteristic	Required Properties	Interested Constituent
<ul style="list-style-type: none"> <li>Satisfy regulatory reporting requirement that the identity of an individual must be clearly established (e.g., IRS requires reporting of social security number)</li> </ul>	<ul style="list-style-type: none"> <li>Include certificate owner identity in such a way that only the intended recipient can access it, or that cannot be changed without detection</li> </ul>	Regulatory Agencies (e.g., IRS, SEC, Dept. of HHS)
<ul style="list-style-type: none"> <li>Preserve the individual's privacy – prevents the cross-linking of different data sources (e.g., address surrogate key problem)</li> </ul>	<ul style="list-style-type: none"> <li>Support limited anonymity</li> <li>Support absolute anonymity</li> </ul>	Certificate owner



## Veiled Certificate

- **Step 1: Apply for Certificate** – Alice (denoted as  $x$ ) sends a request to regulator (or CA)  $j$  to request her  $i$ th certificate. The message contains the owner's identification  $ID_x$ , the owner's certificate-specific public key  $K_{x_i}$ , an encrypted version of these two items  $vct_{x_i} = E_{k_i^{-1}}\{ID_x || K_{x_i}\}$  (hereafter referred to as the VC token), the public key  $k_i$  that allows CA to verify  $vct_{x_i}$ , any additional evidence  $CR_x^j$  needed to prove Alice's credential worthiness to CA  $j$ , along with a digital signature  $DS_{x_i}$  of the entire message signed by Alice.

$$x \rightarrow j: E_{k_j} \{ ID_x || K_{x_i} || vct_{x_i} || k_i || CR_x^j || DS_{x_i} \}$$



## Veiled Certificate

- **Step 2: Regulator Validates Certificate Request** – CA  $j$  validates credentials, and verifies the VC token using the embedded public key,  $k_i$ :

$$D_{k_i} \{ vct_{x_i} \} = D_{k_i} \{ E_{k_i^{-1}} \{ ID_x || K_{x_i} \} \} = ID_x || K_{x_i}$$



## Veiled Certificate

- **Step 3: Regulator creates Veiled Certificate** - Once CA is satisfied with the credentials,  $CR_j$ , and  $DS_j$  are removed and CA digitally signs the certificate with its private key  $K_j^{-1}$ , yielding:

$$VC_{x_i}^j = K_{x_i} \parallel vct_{x_i} \parallel E_{K_j^{-1}}\{ MAC(K_{x_i} \parallel vct_{x_i}) \}$$

CA privately keeps the  $ID_x$  and  $vct_{x_i}$  pair in a list which allows the regulator to use the embedded token to identify the owner of a VC during the lifetime of the VC.



## Veiled Certificate

- **Step 4: Validation of Veiled Certificate** – Veiled certificate is validated by authenticating CA's digital signature. Certificate owner proves ownership by using a challenge response process to verify access to the certificate's private key.



## Veiled Certificate

- **Step 5: Aggregation and Validation of Multiple Veiled Certificates** - Alice can aggregate multiple VCs obtained from different CAs to generate a single certificate with all desired endorsements. A common  $vct_{x_i}$  and  $K_{x_i}$  used by multiple regulators allows aggregation. The resulting aggregated veiled certificate (AVC) is:

$$AVC_{x_i} = K_{x_i} \parallel vct_{x_i} \parallel \bigcup_j E_{K_j^{-1}}\{ \text{MAC}(K_{x_i} \parallel vct_{x_i}) \}, \\ j = 1, \dots, m.$$



## Key Management

- An individual can use one VC with each organization to make his/her data or transactions with different organizations unlinkable.
- However, doing so requires the individual to manage multiple keys, one for each VC.
- Certificate key management can be accomplished either remotely through an ASP service, or locally using a personal key escrow scheme.



# Key Management

- **Using ASP service:** the user authenticates herself with the ASP server, and the server displays a menu for the user to manage. The VC's private keys should be stored in encrypted form for safety reason.
- **Using key escrow scheme:** let the VC embed the matching private key  $K_{x_i}^{-1}$  for the certificate specific key  $K_{x_i}$ , encrypted with certificate owner's symmetric secret key,  $s_x$ . The resulting certificate would be:

$$AVC_{x_i} = K_{x_i} \parallel vct_{x_i} \parallel \bigcup_j E_{K_j^{-1}}\{MAC(K_{x_i} \parallel vct_{x_i})\} \parallel E_{s_x}\{K_{x_i}^{-1}\}, j = 1, \dots, m.$$



# Certificate Properties

Feature	Traditional Non-Digital	Conventional Digital (X.509)	Blind	Fair Blind	Veiled
Uses	Driver's License, Passport	Certification of Public Keys	Digital Currency (eCash)	Revocable Certifiable Credentials	Social Security Certificate
Prevent Certificate Counterfeiting	Limited <sup>1</sup>	Yes	Yes	Yes	Yes
Detect Collusion (sharing of certificate)	Yes <sup>2</sup>	Yes <sup>2</sup>	Yes <sup>2</sup>	Yes <sup>2</sup>	Yes <sup>2</sup>
Prevent Pooling (combine different people's certifications)	Yes	Yes	No	No	Yes
Support Aggregation (combine your own certifications)	Yes	Yes	No	No	Yes
Support Revocation	Yes	Yes <sup>3</sup>	No	Yes	Yes



## Certificate Properties

Feature	Traditional Non-Digital	Conventional Digital (X.509)	Blind	Fair Blind	Veiled
Support Audit Trail	Yes	Yes	No	No	Yes
Support Accountability	Yes	Yes	No	Yes	Yes
Satisfy Regulatory Reporting Requirements	Yes	Yes	No	No	Yes
Support Limited Anonymity (someone can break anonymity)	No	No	No	Yes <sup>4</sup>	Yes
Support Absolute Anonymity (no one can break anonymity)	No	No	Yes	No <sup>4</sup>	No



## Applications

**Q: So how do VCs improve individual's security and privacy?**

A: The Individual has multiple certificates, and each time he hands one out, he gives a different one. The different organizations have different VCs and can not link them. The CA has direct access to the certificate holders ID from both certificates, so his identity is not hidden from the CA.



## Applications

**Q: Can VCs reduce the need for hospitals and doctors to store patient's Personal IDs?**

A: Under HIPAA regulations, hospitals and Doctor's offices must capture and report personal identification numbers, and at the same time keep this information secure. Replacing these personal identifiers with VCs would mean that reporting requirements can still be satisfied, while capturing identifiers that can not cross link records in independent information systems, reducing the risk in case there is a security breach.



## Applications

**Q: Can a bad guy use VCs to hide his overseas investments from the IRS?**

A: No. Even though veiled certificates can shield a individual's personal identifiers from third parties, the certificating agent creating the certificate has full and immediate access. Any report they received containing a VC issued by the U.S. government would be traceable back to the individual, much like social security numbers today. In fact an appropriate application of Veiled Certificates is to replace Social Security Numbers with Veiled Social Security Certificates.



## Conclusion

- Unlike current personal identification numbers, they can not be used for unauthorized cross-linking of independent information systems.
- Veiled Certificates allow the aggregation of certificates issued to the same individual while preventing pooling by multiple individuals.
- Can be implemented under standard X.509v3 protocol.